

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-015147**

(43)Date of publication of application : **18.01.2002**

(51)Int.Cl.

G06F 17/60

G06F 15/00

(21)Application number : **2000-266072**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**

(22)Date of filing : **01.09.2000**

(72)Inventor : **TAGAWA KENJI**
HIROTA TERUTO
MATSUSHIMA HIDEKI
INOUE MITSUHIRO
KAMISAKA YASUSHI
HARADA TOSHIHARU
YUGAWA YASUHEI
MIYAZAKI MASAYA
NAKANISHI MASANORI
KOZUKA MASAYUKI

(30)Priority

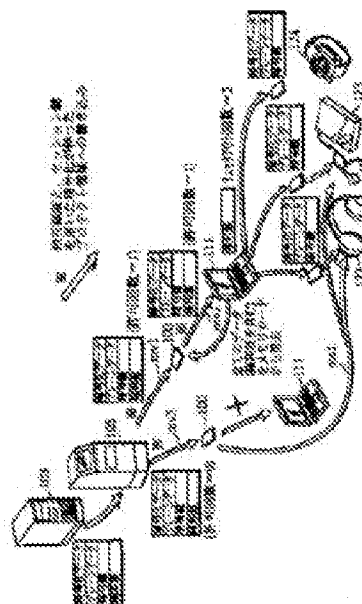
Priority number : 11247922	Priority date : 01.09.1999	Priority country : JP
11258582	13.09.1999	JP
11274182	28.09.1999	JP
2000125864	26.04.2000	JP

(54) DISTRIBUTION SYSTEM, SEMICONDUCTOR MEMORY CARD, RECEIVER, COMPUTER READABLE RECORDING MEDIUM AND RECEIVING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a distribution system capable of realizing high convenience when a device manages check-out/check-in.

SOLUTION: A distribution server 103 distributes contents through a network, a KIOSK terminal 105 receives the contents supply through the network and records the contents on an SD memory card 100. A customer's device 111 receives contents supply through the memory card 100, performs check-out of the contents and records a duplicate on a recording medium. SD-AUDIO players 122 to 124 receive contents duplicate supply and reproduces the contents. In such a case, the KIOSK terminal 105 records a usage rule being the registration certificate of right to manage contents recording on the memory card 100 and sets movement control information showing how many times the right movement is approved in the usage rule.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-15147
(P2002-15147A)

(43) 公開日 平成14年1月18日 (2002.1.18)

(51) Int.Cl. ⁷	識別記号	F I	データベース [*] (参考)
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E 5 B 0 4 9
	Z E C		Z E C 5 B 0 8 j
	1 4 2		1 4 2
	5 1 0		5 1 0
	5 1 2		5 1 2

審査請求 有 請求項の数13 O L (全 46 頁) 最終頁に続く

(21) 出願番号 特願2000-266072 (P2000-266072)

(22) 出願日 平成12年9月1日 (2000.9.1)

(31) 優先権主張番号 特願平11-247922

(32) 優先日 平成11年9月1日 (1999.9.1)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平11-258582

(32) 優先日 平成11年9月13日 (1999.9.13)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平11-274182

(32) 優先日 平成11年9月28日 (1999.9.28)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000003821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 田川 健二

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 廣田 照人

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗 (外1名)

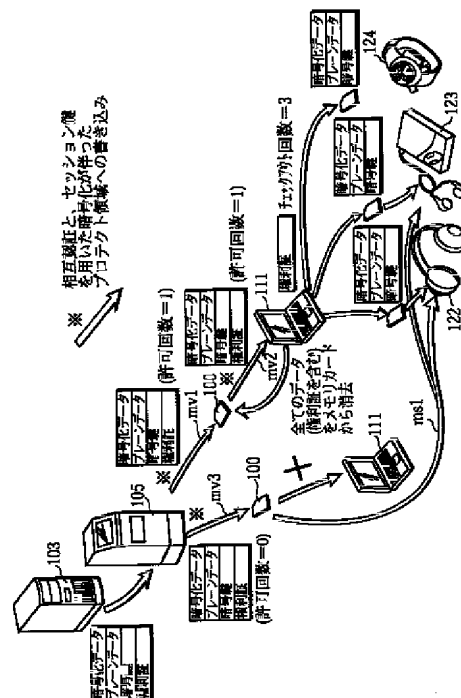
最終頁に続く

(54) 【発明の名称】 配信システム、半導体メモリカード、受信装置、コンピュータ読取可能な記録媒体、及び受信方法

(57) 【要約】

【課題】 機器がチェックアウト チェックインを管理する場合に、高い利便性を実現することができる配信システムを提供する。

【解決手段】 配信サーバ103は、コンテンツをネットワークを介して配信し、KIOSK端末105は、ネットワークを介した前記コンテンツの供給を受けて、コンテンツをSDメモリカード100に記録する。カスタマーズデバイス111は、SDメモリカード100を介したコンテンツの供給を受けて、コンテンツのチェックアウトを行い、複製物を記録媒体に記録する。SD-AUDIOプレーヤ122～124は、コンテンツの複製物の供給を受けて、コンテンツの再生を行う。この際、KIOSK端末105は、SDメモリカード100にコンテンツの記録を管理する権利の権利証であるユーセージルールを記録し、このユーセージルール内に上記権利の移動を何回認めるかを示す移動制御情報を設定する。



【特許請求の範囲】

【請求項1】 コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介してコンテンツを受信する第1、第2受信装置とを含み、受信されたコンテンツの複製物を記録媒体に記録して、再生装置に供給する配信システムであって、

前記第1受信装置は、コンテンツと、記録媒体に対する当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第1受信手段と、

前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセーブル情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備え、

前記第2受信装置は、前記データセットをネットワークを介して配信サーバから受信して、保持する第2受信手段と、

前記配布媒体から許可情報を読み出し、読み出された許可情報に、データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、

第2受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備え、

記録媒体に記録された複製物は、前記再生装置に供給されることを特徴とする配信システム。

【請求項2】 前記配信システムにおいて前記管理情報は、チェックアウトが行なえる残り回数を示し、

前記チェックアウト手段は、前記記録媒体と接続する接続手段を有していて、当該接続手段に接続された記録媒体に未だコンテンツの複製物が記録されておらず、前記第2受信手段、又は、前記データセット移動手段に保持されている管理情報が、1以上の残り回数を示している場合、データセット移動手段が保持しているデータセットにおけるコンテンツの複製物を記録媒体に記録するものであり、

前記第2受信装置は更に

接続手段に接続された記録媒体に既にコンテンツの複製物が記録されている場合、接続手段に接続された記録媒体に記録されているコンテンツの複製物を削除するチェックイン手段と、

記録媒体に複製物が記録されれば、チェックアウトの残り回数をデクリメントするよう第2受信手段又はデータセット移動手段に保持されている管理情報を更新し、記録媒体におけるコンテンツの複製物が削除されればチェ

ックアウトの残り回数をインクリメントするよう管理情報を更新する更新手段とを備えることを特徴とする請求項1記載の配信システム。

【請求項3】 前記記録媒体には、自身に固有の識別子が付与されており、

前記チェックアウト手段は

保持しているコンテンツに、固有の識別子を割り当てて、記録媒体に記録する割当部と、

接続手段に接続された記録媒体に固有な識別子を記録媒体から読み出し、これと、割当部により割り当てられたコンテンツの識別子との組みを記憶する記憶部とを備え、

前記チェックイン手段は

既にコンテンツの複製物が記録されている記録媒体が接続手段に接続されたなら、当該記録媒体に固有な識別子と、コンテンツに固有な識別子との組みを読み取る読取部と、

読取部により読み取られた識別子の組みと、記憶部が記憶している識別子の組みとを比較することにより、接続手段に接続された記録媒体に記録されている複製物が、過去に自装置が記録したものと同一であるか否かを判定する比較部と、

過去に自装置が記録したものと同一である場合、接続手段に接続された記録媒体に記録されている複製物を読み出して保持し、その後、記録媒体から複製物を削除する保持部とを備えることを特徴とする請求項2記載の配信システム。

【請求項4】 請求項3記載の前記データセット移動手段は、

前記配布媒体に記録されている許可情報に、データセットの移動を許可しない旨が示されている場合、コンテンツとユーセーブル情報の移動は行わず、再生装置は更に、

前記許可情報に移動を許可しない旨が示されている場合、これに対応するコンテンツを直接配布媒体から再生することを特徴とする請求項3記載の配信システム。

【請求項5】 コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第1受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第2受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおいて、配布媒体として用いられる半導体メモリカードであって、

コンテンツと、ユーセーブル情報とが記録されているボリューム領域を備え、

前記ユーセーブル情報は、記録したコンテンツの記録媒体に対する複製を管理する管理情報と、管理情報及びコンテンツが第2受信装置に移動することを許可する

か否かを示す許可情報とを含むことを特徴とする半導体メモリカード。

【請求項6】 前記コンテンツは、暗号化されたオーディオデータと、暗号化オーディオデータの暗号化に用いられた暗号鍵との組みを含み、

前記ボリューム領域は、半導体メモリカードと接続している機器の正当性が認証された場合のみ、当該機器によりアクセスされる領域であり、ユーセージール情報と、暗号鍵とが記録されているプロテクト領域と当該機器の正当性が認証されるか否かに拘らず、当該機器によりアクセスされる領域であり、暗号化オーディオデータが記録されているユーザデータ領域と、を備えることを特徴とする請求項5記載の半導体メモリカード。

【請求項7】 前記許可情報は、管理情報及びコンテンツの移動が許可されている場合、その許可回数を併せて示すことを特徴とする請求項6記載の半導体メモリカード。

【請求項8】 コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第1受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第2受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおける第1受信装置であって、コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第1受信手段と、前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備えることを特徴とする受信装置。

【請求項9】 ネットワークを介して配信サーバからコンテンツの供給を受けると共に、コンテンツが記録された配布媒体の供給を受けて、コンテンツの複製物を記録媒体に記録する受信装置であって、前記コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する受信手段と、前記管理情報と、前記データセットを受信装置に移動することを許可するかを示す許可情報とを含むユーセージール情報が記録されており、尚且つ、ユーセージール情報に含まれる許可情報に、前記データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内サブステップへのデータセットの移動を行い、データセットを保持するデータセット移動ステップと、受信ステップ及びデータセット移動ステップの何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセ

ら装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備えることを特徴とする受信装置。

【請求項10】 コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第1受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第2受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおいて、第1受信装置としての処理をコンピュータに行わせるプログラムをコンピュータ読取可能な形式で記録している記録媒体であって、コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第1受信ステップと、

前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録ステップとからなる手順をコンピュータに行わせるプログラムが記録されていることを特徴とするコンピュータ読取可能な記録媒体。

【請求項11】 ネットワークを介して配信サーバからコンテンツの供給を受けると共に、コンテンツが記録された配布媒体の供給を受けて、コンテンツの複製物を記録媒体に記録する受信処理をコンピュータに行わせるプログラムをコンピュータ読取可能な形式で記録している記録媒体であって、

前記コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する受信ステップと、

前記管理情報と、データセットを受信装置に移動することを許可するか否かを示す許可情報とを含むユーセージール情報が前記コンテンツと共に前記配布媒体に記録されており、尚且つ、ユーセージール情報に含まれる許可情報に、前記データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内サブステップへのデータセットの移動を行い、データセットを保持するデータセット移動ステップと、受信ステップ及びデータセット移動ステップの何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセ

ットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウトステップとからなる手順をコンピュータに行わせるプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項12】 コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第1受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第2受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおいて、第1受信装置に適用される受信方法であって、コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第1受信ステップと、前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーザールール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録ステップとからなることを特徴とする受信方法。

【請求項13】 ネットワークを介して配信サーバからコンテンツの供給を受けると共に、コンテンツが記録された配布媒体の供給を受けて、コンテンツの複製物を記録媒体に記録する受信方法であって、前記コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する受信ステップと、前記管理情報と、前記データセットを受信装置に移動することを許可するか否かを示す許可情報とを含むユーザールール情報が前記コンテンツと共に前記配布媒体に記録されており、尚且つ、ユーザールール情報に含まれる許可情報に、前記データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内サブステップへのデータセットの移動を行い、データセットを保持するデータセット移動ステップと、受信ステップ及びデータセット移動ステップの何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウトステップとからなることを特徴とする受信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子音楽配信(Electronic Music Distribution(EMD))等、デジタル著作物の配信サービスを実現する配信システム、半導体メモリ

カード、受信装置、コンピュータ読取可能な記録媒体、及び受信方法に関する。

【0002】

【従来の技術】配信システムは、配信サーバと、コンテンツの購入を行う機器と、コンテンツの再生を行う再生装置とからなり、世界にはりめぐらされた各種ネットワークを介して、様々な地域に居住する人々に、著作物を購入する機会を与えるものである。ユーザが所有しているパソコンを購入機器として用いた場合、コンテンツの購入は以下の過程を経て行われる。ユーザがパソコンを操作して、配信サーバに購入要求を送信したものとす。購入要求が送信されれば、配信サーバは、ユーザに対して課金を行い、その後、デジタル著作物を送信する。ユーザが操作するパソコンは、こうして送信された著作物を受信して、パソコンのハードディスク(以下HDという)に書き込む。著作物の書き込みが正常に行われれば、著作物の購入は完了したことになる。

【0003】著作物を購入した機器は、チェックアウト・チェックインと呼ばれる処理を実行する。チェックアウトとは、半導体メモリカードやミニディスク等、可搬型記録媒体に著作物(一世代複製物)を記録することをいい、著作物を購入した機器は、3回、4回等、予め決められた回数だけチェックアウトを行うことができる。チェックアウトにより可搬型記録媒体に著作物が記録されれば、上述した再生装置を用いてこの著作物を再生させることができる。しかしチェックアウトが予め決められた回数だけ行われれば、著作物はチェックアウト不可能な状態に設定されることとなる。一方チェックインとは、可搬型記録媒体に記録された著作物(一世代複製物)をパソコンに引き戻す処理であり、チェックアウト不可能な状態に設定された後にチェックインを行えば、再度チェックアウトが可能となる。これらチェックアウト・チェックインは、著作権者の利益を不当に害することのないよう、著作権保護を大前提として運営されている。

【0004】チェックアウト・チェックイン時において、著作権がどのように保護されているかを簡単に説明する。ここで複製物を記録すべき記録媒体には、ユーザの通常の操作では読み出せないような領域に固有の識別子(Media-IDと呼ばれる)が記録されており、チェックアウト時には、その記録媒体に固有なMedia-IDを用いて、コンテンツを暗号化する。仮に悪意を持ったユーザが、チェックアウトによりコンテンツが記録された記録媒体から、他の記録媒体へと、コンテンツのコピーを行ったとしても、コピー先の記録媒体に固有なMedia-IDは、コンテンツの暗号化に用いられたMedia-ID(コピー元のMedia-ID)とは異なるので、正常に復号は行えない。この結果著作権は保護されることとなる。

【0005】ここで現状の配信システムには、ユーザが所有しているパソコンを機器として用いたものの他に、コンビニエンスショップ、レコードショップの店頭や店

内、駅構内に設置されたKIOSK端末を機器として用いたものがある。KIOSK端末を機器に用いた場合、著作物の購入は以下の過程を経て行われる。機器であるKIOSK端末は、ユーザに対して、著作物を記録すべき半導体メモリカードやミニディスク等の可搬型記録媒体を準備させ、この可搬型記録媒体とKIOSK端末とが接続されて、代金が支払れた場合、配信サーバから著作物のダウンロードを行い、可搬型記録媒体に記録する。こうしてKIOSK端末の利用者は、通勤、通学、買い物の途中で、手軽に好みの曲を入手することができる。

【0006】KIOSK端末により半導体メモリカードに著作物が記録された場合、KIOSK端末以外の機器は、KIOSK端末により半導体メモリカードに記録された著作物をチェックインしようとはしない。その理由は以下の通りである。仮に他の機器がチェックインを行えば、チェックインされた著作物に基づいて、更に3回、4回といったチェックアウトが行われることが考えられる。他の機器へのチェックインと、その機器によるチェックアウトとが繰り返されれば、膨大な数の一世代コピーが行われることとなり、ひいては、著作権保護の形骸化を招いてしまう。こうした一世代コピーの増殖を防止する意味で、他の機器へのチェックインは全面的に禁じられている。

【0007】

【発明が解決しようとする課題】ところで、KIOSK端末により購入された著作物の他の機器へのチェックインを全面的に禁じるというのは、著作権保護の観点からは合理的であるが、ユーザにとっての利便性は低いと認識されている。即ち、KIOSK端末にて著作物を購入したユーザにとっては、たとえ自宅にパソコン等の機器を所有していたとしても、そのパソコンでチェックアウト チェックインといった機能を楽しむことができないこととなる。正当な料金を支払ったユーザが、自宅に所有しているパソコンにてチェックアウト チェックインを行えないというのは、ユーザに対する配慮が欠けたものであり、KIOSK端末を利用しようという意欲の消沈を招く恐れがある。

【0008】本発明の目的は、著作物を受信した機器がチェックアウト チェックインを管理するという規約が存在する場合に、著作権保護を図りつつも、高い利便性を実現することができる配信システムを提供することである。

【0009】

【課題を解決するための手段】上述した問題点を解決しつつ上記目的を達成するため、本発明では、著作物の複製物の記録を管理する権利についての権利証であるユーザーズールを”移動”させること提案している。SDMI (Secure Digital Music Initiative)においてこの権利証は、DRMI (Digital Right Management Information)とよばれ、チェックアウトやコピー等を行うにあたっての複製物の世代管理や個数管理は、この権利証に基づいてな

される。この権利証の移動を実現して、上記目的を達成する配信システムは、第1受信装置、第2受信装置を含み、前記第1受信装置は、コンテンツと、記録媒体に対する当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第1受信手段と、前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーザーズール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備え、前記第2受信装置は、前記データセットをネットワークを介して配信サーバから受信して、保持する第2受信手段と、前記配布媒体から許可情報を読み出し、読み出された許可情報に、データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、第2受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備えることを特徴としている。

【0010】

【発明の実施の形態】以降、配信システムについての実施形態について説明する。このシステムは、SDMI、SD-Audio Ver1.0規格、SD-Audio Ver1.1規格に準拠して運営されているものとする。SDMI、SD-Audio Ver1.0規格、SD-Audio Ver1.1規格に準拠している機器を対応機器といい、そうでない機器、即ち、SDMI、SD-Audio Ver1.0規格、SD-Audio Ver1.1規格の何れにも準拠していない機器を非対応機器と呼ぶ。SD-Audio Ver1.0規格は、曲の特殊再生や編集操作等が可能のように、記録媒体に著作物を記録するための規格であり、SD-Audio Ver1.1規格は、このSD-Audio Ver1.0規格と比べて、著作物の移動や著作物のプレビューを可能とするものである。

【0011】図1は、著作物のデータ構造を示す図である。本図に示すように著作物は、暗号化データと、暗号化されないプレーンデータと、暗号化に用いられた暗号鍵と、著作物の記録を管理する権利の証明書とから構成される。暗号化データには、MPEG-AACストリームデータ、JPEG静止画データがあり、プレーンデータには、MPEG-AACストリームデータ、JPEG静止画データの再生を制御するナビゲーションデータがある。一方、この権利証は、チェックアウトを何回許可するかを示すチェックアウト許可情報、著作物の移動を何回許可するかの移動許可回数を示す移動制御情報、コピー制御情報を含む。これら著作物を構成するデータセットが記録媒体に記録される際の態様には、図2(a)～図2(c)に示す3つの態様がある。

【0012】図2(a)は、暗号鍵、権利証抜きで著作物が記録媒体に記録された態様(1)を示す図である。この態様(1)では暗号鍵が存在しないので、暗号化データを復号することは出来ず、著作物の再生は不可能となる。図2(b)は、権利証抜きで著作物が記録媒体に記録された態様(2)を示す図である。態様(2)では、暗号鍵と暗号化データとの組みは揃っているのに、著作物を再生する権利はこの記録媒体上に存在することとなる(著作物の実体的な部分をなす暗号化データ及び暗号鍵の組みを本明細書においてコンテンツという場合もある。また暗号鍵と暗号化データとの組みが記録媒体に記録した状態を“再生権利が記録されている状態”という)。しかし記録を管理する権利証は存在しないので、ここに記録された著作物の暗号鍵及び暗号化データを他の記録媒体に記録することはできない。

【0013】図2(c)は、権利証を含んだ状態で著作物が記録媒体に記録された態様(3)を示す図である。著作物の記録を管理する権利は、この記録媒体を内蔵又は接続している機器に存在することとなる。態様(3)では、著作物の再生のみならず、チェックアウト、チェックイン等により図2(b)に示す状態を他の記録媒体に作り出すことも可能となる。

【0014】続いて、著作物をセキュアに格納することができる配布媒体について説明する。そうした配布媒体の一例として、本実施形態では半導体メモリカード(以下、Secure Digital (SD)メモリカードと称する)を用いるものとする。本図におけるSDメモリカード100は図3(a)に示すような外観形状を有し、長さ32.0 mm、幅24.0 mm、厚さ2.1 mmといった大きさ(切手サイズの大きさ)なので、ユーザはこのSDメモリカード100を指先で把持することができる。SDメモリカード100には、機器との接続のための9本のコネクタが設けられており、側面には、記憶内容の上書きを許可するか禁止するかを操作者が設定することができるプロテクトスイッチ101が設けられている。

【0015】図3(b)は、SDメモリカード100の階層構造を示す図である。本図に示すように、SDメモリカード100の階層構造は、著作物を構成するデータセットをセキュアに格納するよう構成された物理層、FAT (FAT: File Allocation Table, ISO/IEC 9293)に基づき、クラスタを最小単位としてアクセスされるファイルシステム層、著作物を構成する暗号化データ、暗号鍵、プレーンデータ、権利証が格納される応用層からなる。

【0016】図3(c)は、SDメモリカード100における物理層の構成を示す図である。本図に示すように、SDメモリカード100の物理層は、システム領域1、Hidden領域2、プロテクト領域3、AKE処理部4、AKE処理部5、Ks復号化部6、Ks暗号化部7、ユーザデータ領域8からなる。システム領域1は、Media Key Block (MKB)と、Media-IDとを格納した読出専用領域であり、ここに

格納されたMKB、Media-IDを書き換えることはできない。SDメモリカード100が他の機器と接続され、MKBとMedia-IDとが他の機器により読み出された場合、これらを読み出した他の機器が、MKB、Media-IDと、自身が所持しているデバイス鍵Kdとを用いて所定の演算を正しく行えば、他の機器は正しい暗号鍵Kmuを所持することができる。

【0017】Hidden領域2は、正解値となる暗号鍵Kmu、即ち、他の機器が正常なデバイス鍵Kdを用いて正常な演算を行なった場合、得られるべき暗号鍵Kmuを格納している領域である。プロテクト領域3は、暗号鍵及び権利証を格納している。Authentication and Key Exchange (AKE)処理部4、AKE処理部5は、機器とSDメモリカード100との間でチャレンジレスポンス型の相互認証を行って、相手側の正当性を認証し、相手側が不当であれば処理を中断するが、相手側が正当であれば機器とSDメモリカード100との間で暗号鍵(セッション鍵Ks)を共有する。機器による認証は3つのフェーズ(機器側で乱数を発生させ、得られた乱数をKmuを用いて暗号化して、チャレンジ値AとしてSDメモリカード100に送信するChallenge1フェーズ、SDメモリカード100側でこのチャレンジ値AをSDメモリカード100内のKmuを用いて復号化し、得られた値をレスポンス値Bとして機器に送信するResponse1フェーズ、機器側で保持していたチャレンジ値Aを機器側のKmuで復号化して、SDメモリカード100から送信されたレスポンス値Bと比較するVerify1フェーズ)からなる。

【0018】SDメモリカード100による認証は3つのフェーズ(SDメモリカード100で乱数を発生させ、得られた乱数をKmuを用いて暗号化して、この値をチャレンジ値Cとして機器に送信するChallenge2フェーズ、機器側においてこのチャレンジ値Cを機器内のKmuを用いて復号化し、得られた値をレスポンス値DとしてSDメモリカード100に送信するResponse2フェーズ、SDメモリカード100側で保持していたチャレンジ値CをSDメモリカード100側のKmuで復号化して、機器から送信されたレスポンス値Dと比較するVerify2フェーズ)からなる。

【0019】この際、他の機器が不正な暗号鍵Kmuを用いて相互認証を行えば、フェーズVerify1,2において、チャレンジ値Aとレスポンス値Bとの不一致、チャレンジ値Cとレスポンス値Dとの不一致が判定され、相互認証が中断することとなる。逆に相手側の正当性が認証されれば、AKE処理部4、AKE処理部5は、上述したチャレンジ値Aと、チャレンジ値Cとの排他的論理和をとり、これをKmuにて暗号化することにより、セッション鍵Ksを得る。

【0020】Ks復号化部6は、SDメモリカード100と接続された他の機器から、プロテクト領域に書き込むべき暗号鍵、権利証であって、暗号化されたものが出力さ

れた場合、それら暗号鍵、権利証がセッション鍵Ksを用いて暗号化されているものとして、セッション鍵Ksを用いることにより復号を行う。そうして復号により得られた暗号鍵、権利証が本来の暗号鍵、権利証であるとして、プロテクト領域に書き込む。

【0021】Ks暗号化部7は、SDメモ리카ード100と接続された他の機器から、暗号鍵、権利証を読み出す旨のコマンドが出力されると、セッション鍵Ksを用いてプロテクト領域に格納されている暗号鍵、権利証を暗号化した後に、そのコマンドを発行した他の機器に出力する。ユーザデータ領域8は、機器の正当性が認証されるか否かに拘らず、当該機器によりアクセスされる領域であり、暗号化データ、プレーンデータが格納される。プロテクト領域から読み出された暗号鍵が正しい値であれば、ここに格納されている暗号化データは正しく復号されることとなる。プロテクト領域に対するデータ読み書きには、Ks復号化部6による復号化と、Ks暗号化部7による暗号化とが伴うので、プロテクト領域は、SDメモ리카ード100と接続している機器がAKEプロセスを正しく行った場合のみ、当該機器により正規にアクセスされることとなる。

【0022】こうした著作物を構成するデータセットが配置されたSDメモ리카ード100に、他の機器が接続された場合、他の機器はどのようなデータを取得することができるかについて説明する。図4(a)は1つ目のケースであり、プロテクト領域に暗号鍵のみが格納された状態で非対応機器がSDメモ리카ード100に接続された場合を表している。このケースでは、ユーザデータ領域に格納されている暗号化データ、プレーンデータを読み出すことができるが、プロテクト領域にアクセスすることができないため、暗号鍵を取得することはできない。この状態は態様(1)と同様であり、この機器は、SDメモ리카ード100と接続しながらも、再生権利を所持できないので著作物を一切再生することができない。

【0023】図4(b)は2つ目のケースであり、プロテクト領域に暗号鍵のみが格納された状態で対応機器がSDメモ리카ード100と接続された場合を表している。この機器はプロテクト領域に格納されている暗号鍵を、ユーザデータ領域に格納されている暗号化データ、プレーンデータと共に読み出すことができる。こうして、暗号化データ、プレーンデータ、暗号鍵を揃えることができるので、この対応機器は、再生権利を所持することができ、著作物を再生させることができる。しかし、プロテクト領域には、権利証が存在せず、この機器は、権利証を読み出すことができないので、この著作物の記録を管理する権利を掌握することはない。

【0024】図4(c)は3つ目のケースであり、プロテクト領域に権利証及び暗号鍵が格納された状態で対応機器が接続され、権利証が、移動を1回許可する旨を示す移動制御情報を含んでいる場合を表している。プロテ

クト領域に含まれる権利証が、1回の移動を許可する旨の移動制御情報を含んでいるので、機器は、権利証ごと著作物をSDメモ리카ード100から読み出し、自身が内蔵している記録媒体に格納しておくことができる。機器が権利証を内蔵記録媒体に記録した状態では、内蔵記録媒体とSDメモ리카ード100とに著作物が存在しており、また権利が二重に発生していることとなるので、機器は著作物を、SDメモ리카ード100から消去するという処理を行う。こうした削除により、機器は、管理権と共に著作物をSDメモ리카ード100から譲り受けたこととなる。

【0025】図4(d)は4つ目のケースであり、プロテクト領域に権利証及び暗号鍵が格納された状態で対応機器が接続され、権利証に含まれる移動許可回数が0回の場合を示す図である。移動制御情報に示される移動の許可回数が0回なので、権利証を移動させることができず、管理権を掌握することはできない。この場合、著作物は、SDメモ리카ード100において著作物の“原盤”のように扱われることとなる。許可回数が“0”となるケースは、元々、移動許可回数は1以上の値であったが、機器の移動が何度か行われ、移動許可回数のデクリメントが繰り返されたため、“0”になった場合に生じる。

【0026】以上でSDメモ리카ード100の構成についての説明を終える。続いて、EMDにおける機器についての説明する。EMDにおける機器には、配信サーバー、デジタルターミナル(第1受信装置)、カスタマーズデバイス(第2受信装置)、SD-AUDIOプレーヤー122~124(再生装置)といった4つの種別があり、以降これらを順に説明する。本実施形態に係る配信サーバー及びデジタルターミナルのうち代表的なものを図5~図6(b)に示し、本実施形態におけるカスタマーズデバイスのうち、代表的なものを図7(a)、再生装置のうち、代表的なものを図7(b)に示す。

【0027】図5における配信サーバー103は、複数の著作物を構成するデータセットを記憶しており、それらのうち、何れかのものの購入がデジタルターミナルやカスタマーズデバイスから申し出されると、購入の申出があった著作物をネットワークを介して、デジタルターミナルやカスタマーズデバイスに送信する。図5、図6(a)、図6(b)におけるデジタルターミナル104~110は、対応機器の1つであり、ネットワークを介して音楽会社が運営している配信サーバー103から著作物を構成するデータセットを譲り受け、SDメモ리카ード100に記録する。ここでネットワークには、ISDN、PSTN等の有線ネットワーク、衛星放送回線、セルラーシステム等、様々な形態の無線ネットワークを含み、デジタルターミナル104~110には、駅や空港の構内や、レコードショップ、コンビニエンスショップの店頭に設置されたKIOSK端末104~108、無線セルラーシステムにて通信を行う携帯電話機109、衛星放送受

信用のSTB110等の種別がある。図5は、駅構内、店頭にKIOSK端末104～108が設置されている様子を示す図である。図6(a)は、携帯電話機タイプのデジタルターミナル109により、著作物を構成するデータセットがSDメモ리카ード100に書き込まれる様子を示す図であり、図6(b)は、STBタイプのデジタルターミナル110により、著作物を構成するデータセットがSDメモ리카ード100に書き込まれる様子を示す図である。KIOSK端末104～108は、専用の光ファイバー回線を介して配信サーバー103と接続されており、上述したデータセットの譲り受けをこの専用回線を介して行う。携帯電話機109は、セルラーシステムに設置された無線基地局、交換局を介して上述したデータセットの譲り受けを行い、STB110は、通信衛星や専用の光ファイバー回線を介して、データセットの譲り受けを行う。

【0028】これらの図におけるデジタルターミナルは、配信サーバー103をアクセスすることにより、配信サーバー103内の記録媒体に格納されている複数の著作物を操作者に提示し、何れかの著作物の購入指示を操作者から受け付ける。操作者が何れかの著作物の購入を行う旨の操作を行えば、その著作物を構成するデータセットの送信を要求する旨の要求信号を配信サーバー103に送信する。配信サーバー103から、著作物を構成するデータセットが送信されれば、デジタルターミナルはそれらを受信して保持し、その後、これらをSDメモ리카ード100に記録する。

【0029】カスタマーズデバイス111～121は、ローカルストレージと呼ばれる記録媒体を内蔵して、ネットワークルート、SDメモ리카ードルート(SDメモ리카ード100を介した著作物の取得ルート)で取得した著作物からなるホームライブラリの管理を行い、SDメモ리카ード100又はローカルストレージに記録された著作物の再生やチェックアウトを行う。図7(a)は、様々なタイプのカスタマーズデバイスを示す図であり、図7(b)は、様々なタイプのSD-AUDIOプレーヤを示す図である。本図において、カスタマーズデバイスは、パソコンタイプのもの(111～116)、民生音響機器タイプのもの(117～121)等様々なタイプがあるが、ローカルストレージを内蔵し、ホームライブラリの管理という点で共通している。ローカルストレージとは、プロテクト領域と、ユーザデータ領域を含み、図4に示したような態様で、著作物を構成するデータセットをセキュアに格納することができる記録媒体である。以降、パソコンタイプのものを一例にして、カスタマーズデバイスの機能について説明する。

【0030】先ず初めにネットワークルートにて、カスタマーズデバイスがどのように著作物を取得するかについて説明する。図8(a)は、ネットワークに接続された配信サーバー103と、複数のユーザが所有するカス

タマーズデバイス(パソコン111～116)とを示す図である。カスタマーズデバイス111は、デジタルターミナル同様、ネットワークを介して配信サーバー103をアクセスし、複数の著作物のうち、何れかのものを取得してローカルストレージに蓄積する。

【0031】ネットワークルートで著作物の構築を繰り返すことにより、ローカルストレージにホームライブラリを構築することができ、著作物の権利証に基づいて、各著作物のチェックアウト チェックインを管理する。図8(b)、図8(c)は、3回という範囲でカスタマーズデバイス111がチェックアウト チェックインを行う様子を示す図である。即ち、権利証にチェックアウトが可能か旨が示されており、その上限数が設定されているなら、その上限数の範囲内で、チェックアウトを行う。この際の動作は以下の通りである。カスタマーズデバイス111にSDメモ리카ード100が接続され、チェックアウトを行う旨が指示されれば、SDメモ리카ード100のプロテクト領域に、暗号化データと、プレーンデータとを書き込む。また、プロテクト領域には、著作物における暗号鍵を書き込む。その後Check-Out回数をデクリメントする。3つのSDメモ리카ード100に著作物を構成するデータセットが記録され、デクリメントによりCheck-Out回数が"0"になると、カスタマーズデバイス111は、図8(c)に示すように、ローカルストレージに格納されている暗号鍵、プレーンデータ、暗号化データをチェックアウト不可能な状態に設定する。

【0032】この際、チェックアウトによりSDメモ리카ード100に著作物を構成するデータセットが記録されたので、対応機器は、SDメモ리카ード100と接続することにより、著作物を再生することができるが、それらを別の記録媒体にコピーすることはない。何故なら、対応機器は、権利証を有していないSDメモ리카ード100からは、暗号鍵を読み出して、自分の記録媒体や、他の記録媒体に記録するという動作は行わないからである。仮に非対応機器がかかる読み出し及び記録を行おうとしても、そうした非対応機器はプロテクト領域をアクセスすることができず(図4(a)参照)、暗号鍵及び権利証の入手には、失敗するので、実質、SDメモ리카ード100に記録された権利証抜ききの著作物が他の記録媒体に記録されることはない。以上のことから、カスタマーズデバイスからSDメモ리카ード100への一代コピーは認められるが、カスタマーズデバイスにより著作物が記録されたSDメモ리카ード100から他の記録媒体への二世コピーは禁止されることとなる。二世コピー以降を禁ずることにより、コピーが無尽蔵に行われるのを禁じている。

【0033】続いてSDメモ리카ードルートにて、カスタマーズデバイスがどのように著作物を取得するかについて説明する。図9は、本実施形態に係るトラック配信システムに含まれる配信サーバと、複数の機器と、再生装

置とを示す図であり、SDメモ리카ードルートにて、カスタマーズデバイス111が著作物を取得する様子を表している。SDメモ리카ード100における著作物の取得処理は以下の通りである。矢印mv1に示すように、SDメモ리카ード100に記録されている著作物の権利証が移動を1回以上許可する旨の移動制御情報を含んでいる場合、カスタマーズデバイス111は、矢印mv2に示すようにSDメモ리카ード100から著作物を構成するデータセットを読み出して、内蔵しているローカルストレージに記録する。その後、著作物を構成するデータセットをSDメモ리카ード100から削除する。SDメモ리카ード100からの取り込みと、著作物の削除とを行うことにより、ネットワークルートで著作物を取得したのと同じ状況をカスタマーズデバイス内に作り出すことができ、以降、カスタマーズデバイスは権利証に従って、チェックアウトを行うことができる。一方、矢印mv3に示すように、SDメモ리카ード100に記録されている著作物の権利証が、移動を0回許可する旨の移動制御情報を含んでいる場合、カスタマーズデバイス111は、SDメモ리카ード100から著作物を構成するデータセットを読み出

ネットワーク -----> SDメモ리카ード -----> ローカルストレージ
 "許可回数:2回" "許可回数=1回" "許可回数=0回"

更に配信サーバー103により"移動許可回数=2回"と設定された権利証をネットワークルートで、カスタマーズデバイスが取得した場合には、移動制御情報に示される移動許可回数は以下のように更新されながら、権利証は

ネットワーク -----> ローカルストレージ -----> SDメモ리카ード
 "許可回数:2回" "許可回数=1回" "許可回数=0回"

これからもわかるように、権利証をネットワークルートで取得する場合、移動許可回数が3回に設定されていれば、カスタマーズデバイスから他のローカルストレージへの権利証の移動が可能となる。SDメモ리카ード100

ネットワーク -----> ローカルストレージ -----
 "許可回数=3回" "許可回数=2回"

----->SDメモ리카ード -----> ローカルストレージ
 "許可回数=1回" "許可回数=0回"

SD-AUDIOプレーヤ122～124は、カスタマーズデバイスがチェックアウトを行うことにより可搬型記録媒体に記録された暗号化データを再生する。SD-AUDIOプレーヤ122はヘッドフォンタイプ、SD-AUDIOプレーヤ123は携帯機器タイプ、SD-AUDIOプレーヤ124はリストバンドタイプであり、ユーザは、通勤や通学の途中で、これらに記録された暗号化データを再生させることができる。図9の一例において、カスタマーズデバイス111に、著作物を構成するデータセットが移動すれば、カスタマーズデバイス111は、権利証に記載に基づいて、例えば3つの可搬型記録媒体に、暗号化データ及び暗号鍵をチェックアウトする。このように3つの可搬型記録媒体に暗号化データ及び暗号鍵がチェックアウトさ

すということは行わない。矢印ms1に示すように、カスタマーズデバイスを介することなく、このSDメモ리카ード100は直接SD-AUDIOプレーヤ122、SD-AUDIOプレーヤ123、SD-AUDIOプレーヤ124に装填され、再生されることとなる。こうやって著作物の権利証を移動させない場合は、著作物の販売価格を安くしてもよい。

【0034】図9において配信サーバー103により"移動許可回数=1回"と移動制御情報が設定された場合には、移動制御情報に示される移動許可回数は以下のように更新されながら、権利証は各記録媒体間を移動してゆくこととなる。

ネットワーク -----> SDメモ리카ード
 "許可回数=1回" "許可回数:0回"

また配信サーバー103により"移動許可回数=2回"と設定された場合には、移動制御情報に示される移動許可回数は以下のように更新されながら、権利証は各記録媒体間を移動してゆくこととなる。

【0035】

各記録媒体 (SDメモ리카ード100、ローカルストレージ) 間を移動してゆくこととなる。

【0036】

を介した著作物の移動は可能であるが、ローカルストレージからローカルストレージへの直接移動は、認められないことは注意すべきである。

れば、SD-AUDIOプレーヤ122～124は、これらを再生させることができる。

【0037】以上でEMDにおける機器についての説明を終える。続いて、著作物を構成するデータセットの詳細について説明する。先ず初めに配信サーバー103からデジタルターミナルへと著作物が伝送される際、著作物はどのようなフォーマットで伝送されるか、即ち、流通時における著作物のデータ構造について説明する。流通時において、曲のような単体の著作物は、パッケージという単位で指示され、また音楽アルバムのような著作物の集合体は、タイトルという単位で指示される。タイトル及びパッケージのデータ構造を示したのが図10であり、以降、タイトル及びパッケージのデータ構造を図1

0を参照しながら説明する。本図において、タイトルは、1つ以上のパッケージ#1, #2 … #Nからなる。各パッケージは、配信可能なファイルであり、1つのヘッダ、Navigation Structure、複数のContent Element(CEL#1, #2, #3 …)、Default Offerを含む。

【0038】『Navigation Structure』は、各CELをどのように再生させるかという再生制御手順を示したデータである。例えば、図10の一例では、CEL#1の再生時にCEL#3の静止画(ピクチャオブジェクト)を表示する旨がこのNavigation Structureに示されることとなる。

『CEL』は、メディア毎に分類された著作物を構成する情報要素である。著作物は曲であるので、著作物は、その曲についての音声と、曲を再生する際、共に表示すべきプロモーション画像等からなり、パッケージは、これらをメディア毎のCELとして格納する。図10の三段目は、CELの一例を示す。CEL#1は、ある曲の音声をエンコードすることにより得られたMPEG-AACストリームデータであり、CEL#2は、CEL#1であるMPEG-AACストリームデータを2秒間隔で頭出ししてゆく際のデータ間隔を示すタイムサーチテーブル、CEL#3は、CEL#1を再生する際、バックグラウンド映像として表示すべきJPEG静止画データである。このように、ある曲についてのメディア毎の情報は、個々のCELとしてパッケージ内に格納されていることがわかる。これらのうち、AACストリームデータ、静止画データは、著作権保護の観点から暗号化され、暗号化データとしてパッケージ内に収録される。

【0039】『Default Offer』は、著作物を販売する際に適用すべき商業的な取り決めを示す情報であり、その販売にあたって購入に対する課金額や著作物に含まれる暗号化データを復号するための暗号鍵等を含む。図11は、Default Offerのデータ構造を階層的に示す図である。本図においてDefault Offerは、『Offer Header』と、『CEL Keychain』と、この著作物の記録を管理する権利についての権利証である『Digital Right Management(DRM)』とを含む。CEL Keychainの内部構成を、破線の引き出し線Df1に引き出して示す。この引き出し線Df1によれば、CEL Keychainは、CEL Keychainについてのヘッダ(CEL Keychain Header(CKH))と、CEL Keychainについての属性を示すCK_ATRと、同じパッケージに含まれるCELを復号するための暗号鍵であるCEL Key(CK)#1, #2, #3, #4 … #nとからなる。

【0040】DRMの内部構成を、破線の引き出し線Df2に引き出して示す。DRMは、本著作物をSDメモ리카ード100に記録した際、SDメモ리카ード100からローカルストレージへの移動を許可するか、許可しないかを示す『Move Control Information(MVCNTI)』、著作物がローカルストレージに移動した際、このカスタマーズデバイスのチェックアウトを何回許可するかを示す『Check-Out Control Information(COCNTI)』と、この著作物の再生をどのような条件で許可するかを示す『Permitted Pl

ayback Count(PB_COUNT)』と、コンテンツ配信業者のIDが記述される『PPDRM_FR_ID1~4』とからなる。

【0041】MVCNTIの詳細設定を破線py1にて引き出して示す。00hに設定された際、SDメモ리카ード100からローカルストレージへの移動は許可されていない旨を示し、01hに設定された際、SDメモ리카ード100からローカルストレージへの移動は一度だけ許可されている旨を示す。MVCNTIに示される移動許可回数は、このパッケージを受信したデジタルターミナルにより、“1”減じられた後、デジタルターミナルによりSDメモ리카ード100に記録されることとなる。

【0042】COCNTIの詳細設定を破線py2にて引き出して示す。001に設定された際、著作物のチェックアウトを一回だけ(1つの記録媒体に対してのみ)許可している旨を示す。002に設定された際、著作物のチェックアウトを2回だけ(2つの記録媒体について)許可し、003、004に設定された際、3つ、4つの記録媒体に対してチェックアウトを許可する旨を示す。

【0043】PB_COUNTの詳細設定を破線py3にて引き出して示す。PB_COUNTは著作物を何秒再生すれば、著作物が1回再生されたかカウントするかを示すPlayback Time(Playback Time)と、著作物の再生を何回許可するかを示すPlayback Counter(Playback Counter)とからなる。続いて、著作物がSDメモ리카ード100に記録される際、著作物を構成するデータセットがどのようなデータ構造に変換されるかについて説明する。SDメモ리카ード100への記録時において、曲等、単体の著作物は、トラックという形態に変換されてSDメモ리카ード100に記録される。トラックは、暗号化されたオーディオデータであるAudio Object(AOB)、暗号化された静止画データであるPicture Object(POB)、トラックについての再生制御情報であるTrack Information(TKI)を含み、著作物を構成する全てのデータは、種別を問わずトラックという単位で一律に管理されることとなる。

【0044】また音楽アルバム等の著作物の集合体は、トラックシーケンスという形態に変換されて、SDメモ리카ード100に記録される。トラックシーケンスは、複数のトラックと、それらトラックの再生順序を定義するプレイリストとからなる。SDメモ리카ード100において、著作物をトラック、トラックシーケンスとして管理するためのデータ構造を図12に示す。図12は、著作物のデータセットを記録するために形成されるファイル、ディレクトリを示す図である。本図における矢印PF1, 2, 3, 4, 5, 6, 7は、パッケージに含まれる各データと、応用層の各ファイルとの対応関係を示す。

【0045】本図においてユーザデータ領域には、Root、SD_Audio、SD_ADEXTディレクトリといった3つのディレクトリが形成されている。このうち、SD_AudioディレクトリはSD-Audio Ver1.0規格に規定されたデータ、SD_ADEXTディレクトリは、SD-Audio Ver1.1規格に固有

のデータを格納するディレクトリである。そのため、SD-Audio Ver1.0規格に対応する機器は、SD_Audioディレクトリに対してアクセスを行うが、SD_AEXTディレクトリに対してアクセスは行わない。一方、SD-Audio Ver1.1規格に対応する機器は、SD_Audioディレクトリ、SD_AEXTディレクトリの双方に対してアクセスを行う。尚、図中のxxxは、001から999までの整数値を示す。

【0046】以降、SD_Audioディレクトリに配置されているファイルを順に説明してゆく。本図に示すように、SD_Audioディレクトリには、『AOBxxx.SA1』『POBxxx.SP1』『SD_AUDIO.TKM』『SD_AUDIO.PLM』『POB000.POM』といった5種類のファイルが配されている。『AOBxxx.SA1』は、パッケージに含まれる複数のCELのうち、AACストリームデータをAOBとして収録しているファイルである。『AOBxxx.SA1』における拡張子『SA』は、『Secure Audio』の略であり、これらの格納内容は、著作権保護の必要性があることを示す。

【0047】続いてAOBファイルの内部構成について説明する。図13は、AOBファイルのデータ構成を階層的に示す図である。本図の第1段目は、AOBファイルを示し、第2段目は、AOBを示す。第3段目は、AOB_BLOCKを示し、第4段目はAOB_ELEMENT、第5段目は、AOB_FRAMEを示す。図13の第5段目における『AOB_FRAME』は、AOBを構成する最小単位であり、再生時間が約20ミリ秒となる可変符号長データである。

【0048】第4段目に位置する『AOB_ELEMENT』は、再生時間が約2秒となる可変符号長データであり、そのデータ長がタイムサーチテーブルに示されている。第3段目に位置する『AOB_BLOCK』は、AOBの先頭部分、又は、終端部分に無効部分が存在する場合、それら無効部分を除いて有効部分のみを指示するデータであり、TKIの中のBITにて指定される。

【0049】第2段目に位置するAOBは、8.4分の再生時間を上限としたデータである。各AOBを8.4分の再生時間に限定した理由は、AOBに含まれるAOB_ELEMENTの個数を制限することにより、タイムサーチテーブルのサイズを504バイト以下に抑制するためである。以下、再生時間の限定により、タイムサーチテーブルの抑制が可能となった理由を詳細に説明する。

【0050】順方向サーチ再生、逆方向サーチ再生の再生を行う際、2秒分読み出しをスキップして240ミリ秒だけ再生するという『2秒スキップ240ミリ秒再生』が行われる。このように2秒という時間長をスキップする場合、その2秒間隔の読出先アドレスをタイムサーチテーブルに記述して、順方向サーチ再生及び逆方向サーチ再生が命じられた際、再生装置がこれを参照すればよい。2秒に相当するデータ長がどの程度になるかについて考察すると、オーディオデータの再生時のビットレートは、上述したように16Kbps～144Kbpsの範囲であるので、2秒当たりに再生されるデータ長は4Kbyte(=16Kbps

×2/8)～36Kbyte(=144Kbps×2/8)となる。

【0051】2秒当たりのデータ長が4Kbyte～36Kbyteであるなら、オーディオデータのデータ長が記述されるためのタイムサーチテーブル内のエントリーのデータ長は、2バイト(16ビット)必要となる。何故なら、エントリーに16ビット長を割り当てたならば、0～64KByteの数値が記述されることが出来るからである。一方、タイムサーチテーブルの総データサイズを例えば504バイト(これは後述するTKTMSRTのデータサイズである)内に制限する場合を考えると、このタイムサーチテーブル内に設けるべきエントリーは、252(=504/2)個に制限せねばならない。上述したように、エントリーは、2秒毎に設けられるものであるので252エントリーに対応する再生時間は、504秒(=2秒×252)となり、8分24秒(=8.4分)となる。このようにAOB_BLOCKにおける再生時間を8.4分以下に制限したことにより、タイムサーチテーブルのデータサイズを504バイト以下とすることができる。

【0052】図14は、AOBファイルに収録されている各AOB、AOB_BLOCKが連続して再生されることにより、どのような再生内容が再生されるかを示す。第1段目は、ユーザデータ領域における8つのAOBファイルを示し、第2段目は、各AOBファイルに収録されている8つのAOBを示す。第3段目は、それぞれのAOBに含まれる8つのAOB_BLOCKを示す。

【0053】第5段目は、5つのパッケージからなるタイトルを示す。5つのパッケージは、SongA、SongB、SongC、SongD、SongEという5つの曲のそれぞれを示す。破線AS1、AS2、AS3 AS7、AS8は、音楽アルバムの分割部分と、AOB_BLOCKとの対応関係を示し、第4段目は、第5段目の音楽アルバムがどのような単位で分割されるかを示す。

【0054】AOB#4は、30.6分という時間にて再生される曲(SongD)の先頭部分であり、8.4分という再生時間にて再生される。AOB#5、AOB#6に含まれるAOB_BLOCKはSongDの中間部分であり、8.4分という再生時間、AOB#7に含まれるAOB_BLOCKは、SongDの終端部分であり、5.4分という再生時間にて再生される。このように30.6分という再生時間を有する曲は、(8.4分+8.4分+8.4分+5.4分)という単位で分割され、各AOBに含まれていることがわかる。この図からも理解できるように、AOBファイルに含まれる全てのAOBは、再生時間長が8.4分という時間長以内に収められていることがわかる。図15は、図14に示したタイトル(音楽アルバム)を格納した8つのAOBファイルを示す図である。

【0055】『POBXXX.JPG/SP1』は、静止画データを収録したファイルであり、『POBXXX.JPG』『POBXXX.SP1』という2つのPOBXXX.JPGと、POBXXX.SP1の違いは、著作権の有無の相違である。前者は、単にJPEG方式の静止画データを収録したファイルであるのに対して、後者は、静止画の著作権を保護するため、暗号化されている点で

ある(その拡張子のSP1は"Secure Picture"の略であり、著作権保護の必要性があることはこれから明らかである。))。

【0056】『SD_Audio.TKM』は、パッケージのヘッダ、Navigation Structure、タイムサーチテーブルの内容を継承したデータであり、トラックマネージャ(Track Manager)を含む。図16(a)は、Track Managerの構成を段階的に詳細化した図である。即ち、本図において右段に位置する論理フォーマットは、その左段に位置する論理フォーマットを詳細化したものであり、破線に示す引き出し線は、右段の論理フォーマットがその左段の論理フォーマット内のどの部分を詳細化したかを明確にしている。このような表記に従って図16(a)におけるTrack Managerの構成を参照すると、Track Managerは、破線の引き出し線h1に示すように、n個のTrack Information(TKIと略す)#1～#nからなる。これらのTKIはAOBファイルに収録されているAOBを、トラックとして管理するための情報であり、各AOBファイルに対応している。

【0057】図16(a)を参照すると各TKIは、破線の引き出し線h2に示すように、Track_General_Information(TKGI)、アーティスト名、アルバム名、編曲者名、プロデューサ名等、TKIに固有なテキスト情報が記述されるTrack_Text_Information_Data_Area(TKXTI_DA)、8.4秒という再生時間を上限としたタイムサーチテーブル(Track_Time_Serch_Table(TKTMSRT))からなる。

【0058】図17は、TKIと、図14に示したAOBファイル及びAOBとの相互関係を示す図である。図17の第1段目における四角枠はTrackA～Eとからなるトラック列(トラックシーケンス)、図17の第2段目における四角枠はTrack Managerを示し、第3、第4段目は図14に示した8つのAOBファイルを示す。第5段目における8つの枠は、8つのAOBを示す。この8つのAOBファイルは、図14に示した8つのAOBを収録していたものであり、TrackA、TrackB、TrackC、TrackD、TrackEを含む音楽アルバムを形成している。第2段目は、8つのTKIを示す。これらTKIに付与された数値"1","2","3","4"は、各TKIを識別するためのシリアル番号であり、各TKIは、同じシリアル番号001,002,003,004,005～が付与されたAOBファイルと対応づけられている。この点に注意して、図17を参照すれば、TKI#1がAOB001.SA1に対応していて、TKI#2がAOB002.SA1、TKI#3がAOB003.SA1、TKI#4がAOB004.SA1に対応していることがわかる(本図における矢印TA1,TA2,TA3,TA4～は、各TKIがどのAOBファイルと対応しているかを示す。)。このように各TKIは、各AOBファイルに収録されているAOBと、1対1の対応関係を有するので、各TKIには、AOBに固有な情報を詳細に記載しておくことができる。

【0059】TKGIの詳細構成を図16(b)に示す。図16(b)に示すように、TKGIは、『TKI_ID』『TKIN』

『TKI_BLK_ATR』『TKI_LNK_PTR』『TKI_SZ』『TKI_PB_TM』『TKI_AOB_ATR』『TKI_POB_ATR』『TKI_T11_ATR』『TKI_T12_ATR』『TKI_TMSRT_SA』『ISRC』『TKI_APP_ATR』『BIT』『TKI_POB_SRP』からなる。『TKI_ID』には、TKIを一意に識別できるID(本実施形態では2バイトの"A4"というコード)が記述される。

【0060】『TKIN』には、1から999までの範囲のTKI番号が記述される。『TKI_BLK_ATR』には、TKIについての属性が記述される。図17の一例では、それぞれのTKIについてのTKI_BLK_ATRがどのように設定されているかについて説明する。各TKIにおけるTKI_BLK_ATRを参照すれば、TKI#1(AOB001.SA1)、TKI#2(AOB002.SA1)、TKI#3(AOB003.SA1)、TKI#8(AOB008.SA1)という4つの組みは、それぞれが独立したトラックに対応しているので、TKI#1、TKI#2、TKI#3、TKI#8のTKI_BLK_ATRは、『Track』と設定されている。TKI#4におけるTKI_BLK_ATRは『Head_of_Track』と設定され、TKI#7におけるTKI_BLK_ATRは『End_of_Track』と、TKI#5、TKI#6は『Midpoint_of_Track』と設定されていることがわかる。このことは、TKI#4と対応関係を有するTKI#4(AOB004.SA1)はトラックの先頭部と、TKI#5、TKI#6と対応関係を有するTKI#5(AOB005.SA1)及びTKI#6(AOB006.SA1)はトラックの中間部と、TKI#7と対応関係を有するTKI#7(AOB007.SA1)はトラックの終端部であることを意味する。

【0061】このTKI_BLK_ATRを設定することにより、複数のトラックのうち、任意の2つを1つのトラックに統合するという統合編集、1つのトラックを複数に分割するという分割編集が容易に行なえることとなる。トラックの統合を行う際の、TKIの更新について説明する。図18(a)、(b)は、2つのトラックを1つに統合する場合にTKIがどのように設定されるかを示す図である。図18(a)において、TrackCとTrackEとを1つのトラックに統合するという編集操作を操作者が希望しているものとする。これらTrackC、TrackEに対応するAOBがAOB003.SA1、AOB008.SA1に収録されており、それらがTKI#3、TKI#8に対応づけられているので、これらTKI#3及びTKI#8のTKI_BLK_ATRの書き換えが行われる。図18(b)は、TKIのTKI_BLK_ATRの書き換え後を示す図である。図18(a)においてTKI#3、TKI#8のTKI_BLK_ATRはTrackと記載されているが、図18(b)では、TKI#3のTKI_BLK_ATRは『Head_of_Track』に書き換えられ、TKI#8のTKI_BLK_ATRは『End_of_Track』に書き換えられている。このように、TKI_BLK_ATRが書き換えられることにより、TKI#3、TKI#8、これらに対応するAOB003.SA1、AOB008.SA1は、TrackCという1つのトラックとして扱われる。

【0062】トラックの分割を行う際の、TKIの更新について説明する。図19(a)、(b)は、1つのトラックを2つのトラックに分割する場合を想定した図である。本図において、TrackCをTrackC-TrackFという2つ

のトラックに分割するという編集を操作者が希望しているものとする。TrackCをTrackC-TrackFに分割しようすると、TrackFに対応するAOB002.SA1が生成される。図19(a)では、TKI#2が『Unused』に設定されており、分割の結果、図19(b)に示すように『Unused』に設定されているTKI#2は、新たに生成されたAOB002.SA1に割り当てられる。

【0063】『TKI_LNK_PTR』には、当該TKIのリンク先のTKIについてのTKINが記述される。図17において矢印TL4, TL5, TL6に示すように、TrackDを構成する4つのAOBファイルに対応するTKI#4、TKI#5、TKI#6、TKI#7は、各TKI_LNK_PTRが次のTKI_LNK_PTRを指示するよう設定されている。『TKI_SZ』には、TKIのデータサイズがバイト数単位で記述される。

【0064】『TKI_PB_TM』には、TKIに対応するAOBファイルに収録されているAOBにより構成されるトラック(曲)の再生時間が記述される。『TKI_AOB_ATR』には、TKIに対応するAOBファイルに収録されているAOBがどのようなサンプリング周波数でサンプリングされているか、どのようなビットレートで転送されるか、チャンネル数がどれだけであるか等、AOBを生成する際のエンコード条件が記述される。

【0065】『TKI_POB_ATR』は、POBをどのようなで態様で表示させるか(シーケンシャルモード、ランダムモード、シャッフルモードといった態様がある。)、POBの表示と、TKIに対応づけられているAOBファイルの再生とを同期させるか否か(スライドショー、ブラウザモードがある。)が設定されるフィールドである。『TKI_T11_ATR』、『TKI_T12_ATR』は、著作物と共に表示されるべきテキスト情報がどのような種類であるか(ISO646, JISX0201, ISO8859, Music Shift JIS漢字等がある。)を示す『TKI_TMSRT_SA』は、TMSRTの先頭アドレスが記述される。

【0066】『ISRC』には、TKGIにおけるISRC(International Standard Recording Code)が記述される。『TKI_APP_ATR』は、本SDメモリカード100に格納されるアプリケーションのジャンルが音楽ジャンルであるか、カラオケソフトであるか、プレゼンテーションデータであるかが記述される。

【0067】『ブロック情報テーブル(BIT)』は、AOB_BLOCKを管理するテーブルである。図16(b)の右側に、BITの詳細構成を示す。図16(b)に示すように、BITは、DATA_OFFSETフィールドと、SZ_DATAフィールドと、FNs_1st_TMSRTEフィールドと、FNs_Last_TMSRTEフィールドと、FNs_Middle_TMSRTEフィールドと、TIME_LENGTHフィールドとからなる。以下、各構成要素の説明を行う。

【0068】『DATA_OFFSET』には、クラスタ境界から各AOB_BLOCKの先頭までの相対アドレスがバイト単位で記述される。これにより、AOBからAOB_BLOCKまでの間に

無効領域がどれだけ存在するかが表現される。AOBとしてSDメモリカード100に格納されている音楽が、エアチェックして録音された音楽であり、その音楽のイントロの部分にディスクジョッキーの音声が混じっている場合、BITにおけるDATA_Offsetを設定することにより、この不要音声をAOB_BLOCKから除外して再生させないようにすることができる。

【0069】『SZ_DATA』には、各AOB_BLOCKのデータ長がバイト単位で記述される。SZ_DATAとDATA_Offsetとを加算した値をAOBを収録しているファイルサイズ(クラスタサイズの整数倍)から差し引けば、AOB_BLOCKに後続する無効領域がどれだけのサイズであるかを求めることができる。つまり、AOBの後半に、再生不要部分が存在する場合、このSZ_DATAを調整することにより、そのような後半部分の無効部分を再生させないようにすることができる。以上のDATA_OFFSET及びSZ_DATAを操作することにより、AOBの前後を部分削除することが可能となる。

【0070】『FNs_1st_TMSRTE』には、当該AOB_BLOCK中の先頭に位置するAOB_ELEMENTに含まれるAOB_FRAME数が記述される。『FNs_Last_TMSRTE』には、AOB_BLOCKの最後尾のAOB_ELEMENTに含まれるAOB_FRAMEの個数が記述される。『FNs_Middle_TMSRTE』には、先頭と最後尾のAOB_ELEMENTを除くAOB_ELEMENT、即ち、AOB_BLOCKの中間部に位置するAOB_ELEMENTに含まれるAOB_FRAMEの個数が記述される。

【0071】『TIME_LENGTH』は、AOB_ELEMENTの再生期間をミリ秒オーダーの時間精度で記述するフィールドである。TIME_LENGTHフィールドは、16ビット長であり、符号化方式がMPEG-AAC方式やMPEG-Layer3方式であれば、AOB_ELEMENTの再生期間は2秒となるので、TIME_LENGTHには、2000の値が記述される。図20は、AOB_ELEMENT#1~#4からなるAOBが格納されているクラスタ007~クラスタ00Eを示す図である。AOBが図20に示すように格納されている場合に、BITがどのように設定されるかについて説明する。本図におけるAOB_ELEMENT#1~#4は、クラスタ007の途中md0からクラスタ00Eの途中md4迄を占有している。BIT内のSZ_DATAは、矢印sd1に示すようにAOB_ELEMENT#1からAOB_ELEMENT#4の最後までを指示しており、BIT内のDATA_Offsetは、非占有部分ud0のデータ長、即ち、クラスタ007の先頭から、AOB_ELEMENT#1の先頭までの相対値を指示している。BITにより、クラスタ境界からAOB_ELEMENTまでのオフセットが管理されることがわかる。

【0072】『TKI_POB_SRP』は、Default_Playlist情報、PlayList情報により指定された再生順序により再生が行われている時間帯のうち、特定のAOBが再生される再生期間に表示すべきPOBを指定するフィールドである。言い換えれば、Track ManagerはTKI_POB_SRPを設定することにより、トラック毎に表示すべきPOBを指定す

ることができる。

【0073】図21は、Track Managerに含まれるTKI#2～TKI#4についてのTKI_POB_SRPの設定例を示す図である。第1段目は、Track Managerを示し、第2段目は、3つのPOBファイルを示す。第1段目におけるTrack Managerは、8つのTKIを含み、矢印は、それらTKI内のTKI_POB_SRPがどのPOBファイルを参照しているかを示す。矢印に示される参照関係によると、TKI#2,#3,#4のTKI_POB_SRPは、それぞれPOB001、POB002、POB003を指定している。POB001～POB003の内容は、TrackB、C、Dに関連するものであり、これらはどれも各トラックが再生されている期間に再生しないと意味がないので、TKIに含まれるTKI_POB_SRPにより、各トラックが再生されている期間において再生されるよう設定されている。

【0074】以上でTKGIについて説明を終える。続いて、図12の残りのファイルについての説明を引き続き行う。『SD_AUDIO.PLM』は、トラックの複数の再生順序を規定する情報であり、Default_Playlist_Track_Search_Pointer(DPL_TK_SRP)#1,#2,#3,#4 #nを含む。図22は、Default_Playlist情報、TKI、AOBファイルの相互関係を示す図である。本図のDefault_Playlist内のDPL_TK_SRP#1,#2,#3,#4 #8のDPL_TKINは、TKI#1,#2,#3,#4 #8を示している。矢印(1)(2)(3)(4)(8)に示すように各AOBが再生されることになる。次に、Default_Playlist情報におけるDPL_TK_SRPの順序を入れ替えることにより、トラックの再生順序を変更するという編集操作がどう行われるかについて説明する。図23(a)、(b)は、トラックの順序を入れ替える場合を想定した図である。図23(a)におけるDPL_TK_SRP、TKIの設定は、図22と同じである。図23(a)における再生順序は、TrackA、TrackB、TrackC、TrackD、TrackEであるが、図23(b)におけるDefault_Playlist情報では、DPL_TK_SRP#3、DPL_TK_SRP#8についてのDPL_TKINの順序が入れ替えられたので、TrackA、TrackB、TrackE、TrackD、TrackCの順序で再生されることになる。このように、Default_Playlist情報における、DPL_TK_SRPの順序を入れ替えることにより、簡易にトラックの再生順序を変更することができる。

【0075】『POB000.POM』は、POBがTKGIにより指定されているか否か、指定されていればその指定回数等を、各POBの管理情報として示す情報である。以上でSD_Audioディレクトリに配置されたファイルについての説明を終え、続いてSD_ADEXTディレクトリに配置されたファイルについて説明する。SD_ADEXTというディレクトリ名における“SD_AD”は、SD-Audio の略であり、EXTはextensionの略である。すなわち、SD-Audio Ver1.1規格のために拡張されたディレクトリであることを表している。

【0076】『STKxxx.SDT』は、図24の内部構成を有する“セキュアな”トラック情報(Secure Track Inform

ation)である。図24を参照すると、STKIは、256バイトのSecure Track General Information (S_TKGI) と、256バイトのSecure Track TextInformation Data Area (S_TKTXTI_DA) とから構成されることがわかる。なお、STKxxx.SDTファイルと、TKIとを比較すると、TKIに存在していたTKTMSRTがSTKIには、存在しないことがわかる。また互いのTKGIを比較すると、TKIのTKGIに存在していたTKI_TMSRT_SA、BITは、STKGIには存在せず、代わりにS_TKI_FR_ID1～4が存在することがわかる。データ構造の違いは以上の通りである。S_TKI_FR_ID1～4は、ID情報を記述するために設けられたフィールドであり、KIOSK端末ごとのIDや、配信方式のID、あるいはユーザごとのID等が記述される。

【0077】以下、TKIとSTKIとの差について説明する。STKIは、著作物の権利証がSDメモリーカード100からローカルストレージへと移動した際、AOBに付随してSDメモリーカード100からローカルストレージへと移動するという付随性を有している点異なる。STKIの内部には、S_TKI_FR_ID1～4が存在しており、これにKIOSK端末毎のIDや、配信方式のID、あるいはユーザごとのID等が記述されているので、STKIは、配信されたコンテンツの購入証明のように用いられる。

【0078】S_TKIファイルとAOBファイルは、ファイル名の3桁の数字部分を同一とすることによって1対1に対応する。図25は、SD_Audioディレクトリに含まれる3つのAOB#1、AOB#2、AOB#3、2つのPOB001.SP1、POB002.SP1がSD_ADEXTディレクトリに含まれる3つのSTKI001.SDT、STKI002.SDT、STKI003.SDTとどのように対応するかを示す図である。AOB、STKIは、矢印AS1、AS2、AS3に示すように同一のシリアル番号を有するもの同士が対応している。S_TKIファイル中のS_TKI_POB_SRPの設定に基づき、矢印PS1、PS2に示すようにPOBは、各STKIと対応づけられる。すなわち図25の例であれば、STKI002.SDTファイル中のS_TKI_POB_SRPにて、POB001.SP1が指定され、STKI003.SDTファイル中のS_TKI_POB_SRPにて、POB002.SP1が指定される。

【0079】以上でユーザデータ領域に配置されているファイルについての説明を終える。続いて、プロテクト領域に配置されているファイルについて説明する。図12においてプロテクト領域には、『AOBSA1.KEY』、『POBSP1.KEY』が配置されたSD_Audioディレクトリ、『AOBSA1.URM』、『POBSP1.URM』が配されたSD_ADEXTディレクトリが存在する。

【0080】『AOBSA1.KEY』は、AOBを復号するための複数の暗号鍵(TitleKey)を収録している暗号鍵格納ファイルである。これらの暗号鍵は、パッケージのDefault Offerに含まれる複数のCEL Keyのそれぞれと対応している。『POBSP1.KEY』は、POBを復号するための複数の暗号鍵(TitleKey)を収録している暗号鍵格納ファイルである。これらの暗号鍵も、パッケージのDefault Offerに

含まれる複数のCEL Keyのそれぞれと対応している。

【0081】『AOBSA1.URM』は、各AOBに対応づけられた権利証(Usage Rule)を収録した権利証格納ファイルである。図26は、AOBSA1.URMの構成を示す図である。本図においてAOBSA1.URMファイルは、ID情報や、バージョン番号、ファイルサイズといった情報が記述されるヘッダ部である『Usage Rule Manager Information』と、Usage Rule Entry#1,#2,#3 …#n(図中では、n=8)から構成される。

【0082】『POBSP1.URM』は、各POBに1対1に対応づけられた権利証(Usage Rule)を収録した権利証格納ファイルである。対応するデータがPOBである点は、AOBSA1.URMと異なっているが、そのデータ構造は、AOBSA1.URMと同一である。図27は、SD_Audioディレクトリの下にAOBファイルが8つ存在し、これらに対応する暗号鍵がAOBSA1.KEYに8つ収録され、これらに対応するUsage RuleがAOBSA1.URMに8つ収録されている場合、AOBSA1.KEYと、AOBSA1.URMと、AOBファイルとの対応を示す図である。

【0083】暗号化されたAOBファイルは、暗号鍵格納ファイル及び権利証格納ファイルと、以下の一定の規則(1)(2)(3)に基づく対応関係を有する。

(1)暗号鍵格納ファイル及び権利証格納ファイルは、暗号化されたファイルが格納されているディレクトリと同じディレクトリ名に配置される。図27のユーザーデータ領域においてSD_AudioディレクトリにAOBファイルが配されており、暗号鍵格納ファイルもSD_Audioディレクトリに配されている。権利証格納ファイルは、SD_AudioディレクトリのサブディレクトリであるSD_ADEXTディレクトリに配されていることから、この規則に従った、ファイル配置が行われていることがわかる。

【0084】(2)暗号鍵格納ファイル及び権利証格納ファイルには、データ領域におけるAOBファイルのファイル名の先頭3文字と、所定の拡張子「.KEY」「.URM」とを組み合わせたファイル名が付与される。図28

(a)、(b)は、AOBSA1.KEY、AOBSA1.URMと、AOBファイルとの対応関係を示す図である。AOBファイルのファイル名が『AOB001.SA1』である場合、暗号鍵格納ファイルには、矢印nk1,nk2に示すように、この先頭3文字『AOB』と、『SA1』と、拡張子『.KEY』とからなる『AOBSA1.KEY』というファイル名が付与されることがわかる。権利証格納ファイルには、矢印nk3,nk4に示すように、この先頭3文字『AOB』と、『SA1』と、拡張子『.URM』とからなる『AOBSA1.URM』というファイル名が付与されることがわかる。

【0085】(3) AOBファイルのファイル名には、暗号鍵格納ファイル及び権利証格納ファイル内において、そのオーディオオブジェクトに対応するTitle key及びUsage Ruleが何番目に位置するか、即ち、対応するTitleKey及びUsage Ruleの順位を示すシリアル番号が付与され

る。AOBファイルのファイル名には、“001”,“002”,“003”,“004”といったシリアル番号が付与されている。これらのAOBファイル内のシリアル番号は、対応するTitle Key及びUsage Ruleがファイルにおいて何番目に位置するかを意味するので、各AOBファイルを暗号化の際に用いたTitle Key及びUsage Ruleは、同一のシリアル番号を有する『Title Key Entry』『Usage Rule Entry』に存在することとなる。図27における矢印AK1,AK2,AK3,AK4は、AOBファイルとTitleKey、Usage Ruleとの対応関係を示す。

【0086】続いてTitle Key Entryの内部構成について説明する。図29はTitle Key Entryの内部構成を示す図である。図29に示すように、Title Key Entryは、7バイトの暗号鍵『EKEY』、『Availability Flag』、『Content ID』とからなる。『Availability Flag』は、SDメモリーカード100において著作物が存在し、かつ当該エントリに有効な暗号鍵を記述する際、“1”に設定され、著作物がSDメモリーカード100からローカルストレージと移動した際、“0”に設定されるフラグである。

【0087】『Content ID』は、コンテンツごとにユニークに割り振られる情報である。またAvailability Flagは、Content_IDと共に以下のように併用される。空きのTitle Key EntryにおけるContent_IDは“0”、空きでないTitle Key EntryにおけるContent_IDは(空きでないTitle Key Entryとは、Title Key Entryに対応するAOBファイルが存在することをいう。)、1~999と設定される。更にトラックとTKI(AOB)が1対多で対応する場合、AOBに対応するTitle Key EntryにおけるContent_IDが、全て同一の値となる。一方Availability Flagは、トラックとTKI(AOB)が1対1で対応する場合“1”に設定される。トラックとTKI(AOB)が1対多で対応する場合、多くのTitle Key Entryのうち、唯一のもののAvailability Flagが“1”に設定される。残りのTitle Key EntryのAvailability Flagは“0”に設定される。Content_IDが“0”ではなく、Availability Flagが“0”に設定されていれば、同一のContent_IDを有するTKI(AOB)が複数存在し得るから、これをきっかけに同一のContent_IDを有するTitle Key Entryを検出する。そうして1つのContent_IDに対応する複数のTKI(AOB)を特定するというサーチ処理が可能となる。

【0088】続いてUsage Ruleについて説明する。図26の右半分にUsage Ruleの構成を示す。各AOBに対応するUsage Ruleのフォーマットは図26の右半分に表され、『C_HASHフィールド』、『Check-Out Control Information(制御情報)』、『Move Control Information(制御情報)』、『Trigger Bit』、『Content_IDフィールド』、『Availability Flag』、『STI_KEY』からなる。図中の“{”記号にも示されているように、Content ID、Availability Flag、STI_KEYは、図29に示したTitle

Key Entryの構成と同様である。

【0089】『C_HASHフィールド』は、Enc-STKI、Enc-STI_KEY、Enc_AOBを連結して、SHA-1 (Secure Hash Algorithm) に適用することにより得られる演算結果のうち、下位64ビットが書き込まれる(“Enc_”というのは、暗号化がなされているという意味である。)。ハッシュ関数とは一方方向性関数であり、入力値の一部でも変化すると、出力値は大きく異なるという特徴を有する。さらに、入力値から出力値(ハッシュ値)を類推するのは非常に困難という特徴も有する。このC_HASHフィールドに書き込まれた値は、カスタムデバイスがSDメモ리카ード100をアクセスする際、Enc-STKI、Enc-STI_KEY、Enc_AOBが「他のデータ」にすり替えられたか否かの検証に用いられる。

【0090】即ち、SDメモ리카ード100がカスタムデバイスに接続されると、カスタムデバイスはEnc-STKI、Enc-STI_KEY、Enc_AOBを連結して、これを下記のようにSHA-1アルゴリズムに適用し、64ビットのC_HASH-Ref値を得る。このようにして得たC_HASH-Ref値と、Usage RuleのC_HASHフィールドに書き込まれたC_HASHとの照合を行う。Enc-STKI、Enc-STI_KEY、Enc_AOBがデジタルターミナルによりSDメモ리카ード100に記録された時点と同じものなら、C_HASH-Ref値はUsage Ruleに書き込まれているものと同じ値となるが、Enc-STKI、Enc-STI_KEY、Enc_AOBが改竄されたり、他のものにすり返られているなら、算出されるべきC_HASH-Ref値は、Usage Rule ManagerのC_HASHに記載されているものと大きく異なることとなる。このような照合をカスタムデバイスに行わせる目的で、C_HASHフィールドはUsage Rule Managerに設けられている。

【0091】『Check-Out制御情報』は、SDメモ리카ード100がカスタムデバイスに接続され、Usage RuleがSDメモ리카ード100からローカルストレージに移動した際、幾つの記録媒体に、このUsage Ruleに対応するAOB、Title Keyの組みを記録させるかを示す。『Move制御情報』は、SDメモ리카ード100からローカルストレージへの権利移動(記録を管理する権利の移動)が許可されているか否かを示す情報である。“1”に設定された場合、当該権利移動が1回だけ許可されている旨を示し、“0”に設定された場合、許可回数は0回であり、当該権利移動が禁止されている旨を示す。Move制御情報に示される移動許可回数は、このUsage Ruleを有するSDメモ리카ード100と接続したカスタムデバイスにより、“1”減じられた後、カスタムデバイスによりローカルストレージに記録されることとなる。

【0092】『Trigger Bit』は、“0”に設定されれば、権利移動を、Move制御情報のみで判断してよいかを示し、“1”に設定されれば、権利移動の可否は、Move制御情報だけでなく、他の情報を参照して総合的に行うべき旨を示す。Trigger Bitが設けられているのは、将来のU

sage Ruleの機能拡張に備るためである。即ち、著作物の移動の可否を判断するにあたって、Move制御情報だけでなく、他の要件の組み合わせで、判断を行いたいという要望が将来生じるかもしれない。そうした要望が生じた際には、Trigger Bitを“1”に設定しておき、その要件の成立と、Move制御情報の1の設定とが同時に満たされた場合に、著作物の移動を行わせる。

【0093】以上で応用層のデータについての説明を終える。続いて、SDメモ리카ード100からローカルストレージへと著作物の移動が行われる際、これまでに説明したファイルがどのように移動するかについて説明する。図30(a)、(b)は、著作物を構成するデータセットがSDメモ리카ード100からローカルストレージにどのように移動するかを示す図である。ユーザデータ領域に配置されたファイルのうち、AOBファイル、POBファイル、STKIファイルは矢印MY1、MY2、MY3に示すように、SDメモ리카ード100のユーザデータ領域から、ローカルストレージのユーザデータ領域へと読み出されることとなる。その後、SDメモ리카ード100におけるAOBファイル、POBファイル、STKIファイルは、削除されることとなる。一方、SDメモ리카ード100におけるプロテクト領域では、AOBSA1.KEY、POBSP1.KEY、AOBSA1.URM、POBSP1.URMは矢印MY4、MY5、MY6、MY7に示すように、ローカルストレージにおけるプロテクト領域に読み出されることとなる。

【0094】図30(a)、(b)は、SDメモ리카ード100におけるユーザデータ領域のオーディオオブジェクトを全てローカルストレージに移動させるケースを想定していたが、ユーザデータ領域における8つのAOBのうち、3つのみを移動させようとする場合、SDメモ리카ード100のユーザデータ領域にどのようなファイルが配置されるかを図31(a)、(b)に示す。図31

(a)において、SDメモ리카ード100のユーザデータ領域と、プロテクト領域からAOB#1～#3、Title Key Entry#1～#3、Usage Rule Entry#1～#3がユーザデータ領域と、プロテクト領域から削除され、かわって図31

(b)に示すように、ローカルストレージのユーザデータ領域と、プロテクト領域には、AOB#1、AOB#2、AOB#3、Title Key Entry#1～#3、Usage Rule Entry#1～#3が配置されることとなる。

【0095】図32は、図25に示したAOBファイル、POBファイル、STKIファイルがSDメモ리카ード100からローカルストレージへとどのように移動するかを示す図である。本図に示すように、SDメモ리카ード100におけるAOB001.SA1、AOB002.SA1、AOB003.SA1、POB001.SP1、POB002.SP1、STKI001.SDT、STKI002.SDT、STKI003.SDTはSDメモ리카ード100から削除され、かわって、ローカルストレージにこれらのファイルが配置されていることがわかる。以上で、応用層におけるディレクトリ構成、ファイル構成についての説明を終える。ローカルス

トレージにおいて、SDメモリカード100と同様のディレクトリ構造を有しているが、流通時のフォーマットに示したフォーマット、即ち、図10に示したタイトル及びパッケージらなるフォーマットに変換して記憶しておいても良い。続いて、デジタルターミナルの構成について説明する。

【0096】図33は、KIOSK端末型デジタルターミナルの構成を示す図である。本図に示すようにKIOSK端末型デジタルターミナルは、音楽会社からリリースされている著作物からなるホームライブラリを閲覧するためのリリースコンテンツブラウザ部21と、著作物に対する検索操作や著作物についての購入操作を操作者から受け付けるタッチパネル22と、光ファイバー等の専用回線との接続を行い、専用回線を介した著作物の送受信を行う通信部23と、PCMCIAのカードアダプタで構成され、SDメモリカード100との間の入出力を行うカードコネクタ24と、コインペンダを用いた現金受け取りや、キャッシュカード、ICカードを用いたオンライン決済を行うことにより、ユーザに対する課金を行う課金部25と、SDメモリカード100のプロテクト領域をアクセスするにあたって、必要な暗号化処理、復号化処理を実行するセキュア処理部26と、KIOSK端末における販売サービスの統合制御を行う販売サービス制御部27とからなる。

【0097】図34(a)は、パソコン型カスタマーズデバイスの構成を示す図である。デジタルターミナルは、ユーザがKIOSK端末から購入した著作物、ネットワークルートで購入した著作物からなるホームミュージックライブラリを記録するローカルストレージ32と、公衆回線との接続を行い、公衆回線を介して著作物の送受信を行う通信部33と、PCMCIAのカードアダプタで構成され、SDメモリカード100との間のデータ入出力を行うカードコネクタ34と、ホームライブラリに対するブラウザ機能を有するホームライブラリブラウザ部35と、操作者から操作を受け付ける入力受付部36と、ローカルストレージ32に構築されているホームライブラリに新たな著作物を加える処理や、ローカルストレージに含まれる著作物を他の記録媒体にチェックアウトする処理を操作者からの操作に従ってを行うライブラリ管理部37と、SDメモリカード100のプロテクト領域をアクセスするにあたって、必要な暗号化処理、復号化処理を実行するセキュア処理部38とからなる。

【0098】続いてSD-AUDIOプレーヤ122～124の内部構成を、図34(b)を参照しながら説明する。図34(b)に示すように、SD-AUDIOプレーヤ122～124は、PCMCIAのカードアダプタで構成され、SDメモリカード100との間のデータ入出力を行うカードコネクタ60、TitleKeyを用いてAOBファイルの暗号化を解除するデスクランブラ61、AOBファイルを復号することにより、PCMデータを得るAACデコーダ62、AACデコー

ダ62の復号により得られたPCMデータをD/A変換して、ヘッドホン端子を介してスピーカに出力するD/Aコンバータ63、SD-AUDIOプレーヤ122～124の処理を統合する制御部64からなり、カスタマーズデバイスのチェックアウトによってSDメモリカードに記録されたトラック、又は、移動不可と設定されたUsage Ruleと共に、SDメモリカード100に記録されたトラック、移動可能と設定されたUsage Ruleと共に、SDメモリカード100に記録されたトラックを再生する。著作物の再生は、SD-AUDIOプレーヤ122～SD-AUDIOプレーヤ124によりなされるものとして説明したが、カスタマーズデバイス自身に図34(b)の内部構成を具備させて、著作物の再生を行わせてもよい。

【0099】また、デジタルターミナルやカスタマーズデバイスにおける操作者の操作の受け付けは、タッチパネル以外にも、キーボードやマウス、トラックボール、スライドパッド、又はこれらの組み合わせで行ってもよい。更にリリースコンテンツブラウザ部21、ホームライブラリブラウザ部35は、CRTやプラズマディスプレイ、液晶ディスプレイ等で、上述したコンテンツの閲覧を行わせてもよい。

【0100】続いてデジタルターミナルに内蔵されているセキュア処理部26の構成について説明する。図35に示す通りセキュア処理部26は、MKB処理部41、ID処理部42、AKE処理部43、Kmu暗号化部44、STI暗号化部45、Ks暗号化部46からなる。MKB処理部41は、SDメモリカード100のシステム領域に格納されているMKBと、デジタルターミナルの製造メーカーにより付与されたデバイス鍵Kdとを読み出し、これらを用いて所定の演算を行うことにより、56ビットの暗号鍵KmをID処理部42に出力する。

【0101】ID処理部42は、MKB処理部41から56ビットの暗号鍵Kmが出力されれば、SDメモリカード100のシステム領域からMedia-IDを読み出して、所定の演算を行うことにより、64ビットの演算結果を算出し、そのうち下位56ビットを暗号鍵Kmuとして、AKE処理部43及びKmu暗号化部44に出力する。AKE処理部43は、ID処理部42により算出された暗号鍵Kmuと、SDメモリカード100側の暗号鍵Kmuとを用いたAKEプロセスを行う。その結果として得られた56ビットのセッション鍵KsをKs暗号化部46に出力する。

【0102】Kmu暗号化部44は、STI_KEY(図中では、KSTIと表記している)をランダムに選び、そのSTI_KEYを、ID処理部42が出力した暗号鍵Kmuを用いて暗号化してKs暗号化部46に出力する。また、Enc-STKI、Enc-STI_KEY、Enc_AOBを集めて、アルゴリズムSHA-1に適用することにより、C_HASH値を算出する。暗号化されたSTI_KEYと、C_HASH値とが得られると、C_HASH値をUsage Ruleに書き込んで、そのUsage Ruleを暗号鍵Kmuを用いて暗号化してKs暗号化部46に出力する。

【0103】STI暗号化部45は、STI_KEYを用いてSTKIを暗号化し、SDメモ리카ード100に出力し、ユーザデータ領域に書き込ませる。Ks暗号化部46は、AKE処理部43から出力された56ビットのセッション鍵Ksを用いて、STKIとUsage Ruleとの組みを暗号化して、SDメモ리카ード100に出力し、プロテクト領域3に書き込ませる。

【0104】以上で、デジタルターミナルにおけるセキュア処理部26の構成についての説明を終える。続いて、カスタムデバイスにおけるセキュア処理部38の構成について説明する。セキュア処理部38の内部構成は、図36に示す通りであり、MKB処理部51、ID処理部52、AKE処理部53、Ks復号化部54、Kmu復号化部55、STI復号化部56からなる。

【0105】MKB処理部51は、SDメモ리카ード100がカスタムデバイスに接続されると、システム領域1からMKBを読み出し、デバイス鍵Kdを用いて読み出されたMKBに対して所定の演算を行うことにより、56ビットの暗号鍵Kmを得る。ID処理部52は、接続されたSDメモ리카ード100のシステム領域1からMedia-IDを読み出し、MKB処理部51により算出された暗号鍵Kmと、読み出されたMedia-IDとを用いて所定の演算を行い、64ビットの演算結果を得て、そのうち下位56ビットを暗号鍵Kmuとして、AKE処理部53とKmu復号化部55とに出力する。

【0106】AKE処理部53は、Ks復号化部54により出力された暗号鍵Kmuを用いて、SDメモ리카ード100におけるAKE処理部5とAKEプロセスを行い、その結果である56ビットのセッション鍵KsをKs復号化部54に出力する。Ks復号化部54は、プロテクト領域に格納されているEnc-STKIとEnc-Usage Ruleとの組みであって、暗号化されたものをSDメモ리카ード100から読み出し、AKE処理部53が出力した56ビットのセッション鍵Ksを用いて復号する。そしてその結果をKmu復号化部55に出力する。

【0107】Kmu復号化部55は、ID処理部52により算出された56ビットの暗号鍵Kmuを用いて、復号化を行い、STKIとUsage Ruleとの組みを得る。STI復号化部56は、ユーザデータ領域からEnc-STI_KEYを読み出し、AKE処理部53から出力されたSTI_KEYを用いて、読み出されたEnc-STKIの復号化を行って、STKIを得る。

【0108】以上説明したセキュア処理部26、セキュア処理部38による復号化、暗号化はC_CBC(Converted Cipher Block Chaining)モードで行われる。暗号化されたデータが512Byteであるとする、C_CBCモードでは、このデータの8バイト部分を1つのブロックとして扱い、先頭の8バイトのブロックを7バイトの暗号鍵Mkを用いて復号する。その結果得られた8バイトの演算結果を、部分鍵として保持しておき、次の8バイトブロックの復号化に用いる。こうして512Byteのデータは8バイト単位

に、復号化されてゆく。

【0109】また、AKEプロセスによるセッション鍵Ksの共有、SDメモ리카ード100からの暗号化データの読み出し、セッション鍵Ksを用いた暗号化データの復号化、暗号鍵Kmuを用いた暗号化データの復号化といった一連の処理をセキュアリードといい、機器がSDメモ리카ード100に対して所定のリードコマンド(セキュアリードコマンド)を発行した際、これらの処理は順次実行される。

【0110】更に、暗号鍵Kmuを用いた暗号化データの暗号化、AKEプロセスにより得られたセッション鍵Ksを用いた暗号化データの暗号化、暗号化後のデータ送信といった一連の処理をセキュアライトといい、機器がSDメモ리카ード100に対して所定のライトコマンド(セキュアライトコマンド)を発行した際、これらの処理は順次実行される。以上でセキュア処理部26、セキュア処理部38の内部構成についての説明を終える。

【0111】続いて、デジタルターミナル、カスタムデバイスの処理を統合する制御部である販売サービス制御部27、ライブラリ管理部37について説明する。販売サービス制御部27は、デジタルターミナルの統合制御を行うよう記述された実行形式プログラムを記憶したROMと、RAMと、CPUとからなる。この実行形式プログラムの処理手順を記載したのが、図37、図38のフローチャートである。以降、これらのフローチャートを参照しながら、販売サービス制御部27の制御内容について説明する。図37のフローチャートの処理が開始されれば、ステップS1において、販売サービス制御部27は音楽会社からリリースされている著作物を紹介する一覧画面をリリースコンテンツブラウザ部21に表示させた後、ステップS2～ステップS3を繰り返し行うループ処理に移行する。ステップS2では、著作物の購入を求める旨の操作が操作者から行われたかを判定し、ステップS3では、著作物の検索を求める旨の操作が操作者から行われたかを判定する。検索が要求されたなら、ステップS3においてYesとなり、ステップS4に移行する。ステップS4において、アーティスト名、曲名等のキーワード入力をタッチパネル22を介して操作者から受け付け、ステップS5において通信部23を介して、配信サーバー103をアクセスすることにより、キーワードに該当する著作物についての情報を配信サーバー103から検索する。そして、ステップS6において検索された著作物を示す一覧画面をリリースコンテンツブラウザ部21に表示させた後、ステップS2～ステップS3からなるループ処理に戻る。

【0112】操作者により購入が要求されたなら、ステップS2がYesになってステップS7に移行し、課金部25に対する現金支払が行われるのを待つ。硬貨がコインベンダーに投入されたなら、販売サービス制御部27はステップS8において選択された著作物についてのパ

パッケージの送信要求を通信部23に送信させる。その後、ステップS9においてパッケージの受信待ちを行い、ステップS10では、パッケージを正常に受信したかを判定する。正常でなければ、ステップS8に移行し、送信要求を通信部23に再度出力させる。通信部23がパッケージを正常に受信したなら、ステップS11においてパッケージをSD-AudioVer1.1形式に変換しつつSDメモ리카ード100に記録する。ステップS12では、SDメモ리카ード100へのデータ記録が正常に行われたか否かを判定し、否ならば、ステップS14において現金払い戻しを行う。正常に行われたならばステップS13において、課金部25に決済処理を行わせる。その後、ステップS1に移行し、初期画面表示をリリースコンテンツブラウザ部21に行わせて、ステップS2へステップS3からなるループ処理に移行する。

【0113】ステップS11において、SD-Audio Ver1.1形式への変換がどのように行われたかを図38のフローチャートを参照しながら詳細に説明する。SDメモ리카ード100に著作物を記録しようとする場合、SDメモ리카ード100中のユーザ領域のSD_AUDIOディレクトリをアクセスし、AOBxxx.SA1ファイルを読み出し、サーチし、空き番号があるかどうか判定する。もしも、AOBxxx.SA1ファイルがすでに999個存在する場合は、コンテンツをこれ以上記録できない旨を表示し、終了する。999個未満なら、ステップS21において、販売サービス制御部27はパッケージのCELに含まれるAACストリームデータを複数のAOBファイルに分割して、SD-AUDIOディレクトリに記録する。その後、ステップS22において、販売サービス制御部27は、SDメモ리카ード100のユーザデータ領域に格納されているTrack Managerをオープンし、各AOBファイルに対応するTKIをTrack Manager内に生成する。ステップS23では、パッケージに含まれるヘッダ、Navigation Structureに基づいた内容をTrack Manager内の複数TKIに設定する。続いてステップS24において販売サービス制御部27は、静止画データを複数のPOBファイルと、POMとに変換し、SDメモ리카ード100に記録する。ステップS25では、タイムサーチテーブルを分割して、対応するTKI内のTKTMSRTとして設定し、ステップS26において販売サービス制御部27は、Navigation Structureに基づいて、Playlist上におけるDPL_TK_SRPを設定する。以上で、SDメモ리카ード100のユーザデータ領域のSD-Audioディレクトリに配置されるべきデータセットが設定されたこととなる。

【0114】以降、ステップS90に移行して、DRMのMove制御情報に示されるMove許可回数は0であるかを否かを判定する。"0"であれば、ステップS27～ステップS33、ステップS91の処理をスキップしてステップS35に移行し、1つ以上ならステップS27に移行する。次にステップS27において販売サービス制御部27は、Title Key Managerに生成された複数TKIに基づい

て、複数のSTKIを生成する。ステップS28では、複数のSTI_KEYを生成し、これらを用いて各STKIを暗号化した後、SD_ADEXTディレクトリに記録する。ステップS29において販売サービス制御部27は、SDメモ리카ード100からUsage Rule Managerをセキュアリードし、ステップS30において各販売サービス制御部27は、AOBに対応するUsage RuleをUsage Rule Managerに生成する。ステップS91においてMove許可回数のデクリメントを行い、ステップS31において、デクリメントされたMove許可回数と、CheckOut制御情報とを各Usage Ruleに設定する。ステップS32においてSTKIの暗号化に用いたSTI_KEYをUsage RuleのSTI_KEYフィールドに設定する。ステップS33では、SDメモ리카ード100にUsage Rule Managerをセキュアライトする。以上の処理にて、STKI、Usage Rule Managerが記録されたので、SD-Audio Ver1.1規格対応のデータがSDメモ리카ード100に設定されたこととなる。

【0115】続いて、ステップS35では、SDメモ리카ード100からTitle Key Managerをセキュアリードし、ステップS36において販売サービス制御部27は、Default Offer内のCEL Key Chainに含まれるCEL KeyをAOBSA1.KEYの各AOBに対応するTitle Key Entryに書き込む。ステップS37において販売サービス制御部27は、CEL Keyが書き込まれたTitle Key ManagerをSDメモ리카ード100にセキュアライトする。

【0116】以上でデジタルターミナルにおける販売サービス制御部27についての説明を終える。続いてカスタマーズデバイスについてのライブラリ管理部37について詳細な説明を行う。ライブラリ管理部37は、カスタマーズデバイスの統合制御を行うよう記述された実行形式プログラムを記憶したROMと、RAMと、CPUとからなる。この実行形式プログラムの処理手順を記載したのが、図39～図41のフローチャートである。以降、これらのフローチャートを参照しながら、ライブラリ管理部37の制御内容について説明する。図39のフローチャートの処理が開始されれば、ライブラリ管理部37はステップS41においてローカルストレージ32に格納されているトラックの一覧表示を行い、ステップS42～ステップS45を繰り返して行うループ処理に移行する。ステップS42においてライブラリ管理部37は、SDメモ리카ード100からローカルストレージ32へのトラック移動が要求されたかの判定を行い、ステップS43では、トラックのチェックアウトが要求されたかの判定、ステップS44では、トラックのチェックインが要求されたかの判定、ステップS45では、サーバコンピュータからの著作物購入が要求されたかの判定を行う。

【0117】サーバコンピュータからの著作物購入が要求された場合、ステップS45がYesとなってステップS46に移行する。ステップS46においてライブラリ

ィ管理部37は通信部33にダウンロード要求を送信させ、ステップS47においてパッケージの受信待ちを行う。パッケージの受信を行えば、図37のフローチャートに示したデジタルターミナルの処理と同様の処理を行って、ステップS48において受信したパッケージをローカルストレージ32に格納し、その後、ステップS42～ステップS45に移行する。

【0118】SDメモリカード100からローカルストレージ32へとトラックを移動する処理が要求されたなら、ステップS42がYesとなり、図41のステップS71に移行して、ライブラリ管理部37は、SDメモリカード100からUsage Rule Managerをセキュアリードする。以降、このSDメモリカード100において格納されている複数のトラックのそれぞれを変数#xにて指示するものとする。以降、ステップS72において#xに初期値を代入し、ステップS73においてライブラリ管理部37は、Usage Rule#xのTrigger Bitをチェックする。Trigger Bitが“1”なら、次のトラックに処理を移すよう、ステップS79に移行して変数#xをインクリメントした後、ステップS73に移行する。Trigger Bitが“0”なら、ステップS74においてライブラリ管理部37は、Usage Rule#xのMove制御情報をチェックする。Move制御情報に示される移動許可回数が“0”ならそのトラックをローカルストレージ32に移動することは禁じられているので、次のトラックに処理を移すよう、ステップS79に移行して変数#xをインクリメントした後、ステップS73に移行する。Move制御情報が“1”であれば、ステップS75に移行する。

【0119】ステップS75では、Enc-STKI#x、Enc-STI_KEY#x、Enc-AOB#xを連結して、C_HASH-Ref値#xを得る。そして、ステップS76においてライブラリ管理部37は、C_HASH-Ref値#xと、Usage Rule#xにおけるC_HASH#xとが一致か否かを判定する。一致しなければ、ステップS79に移行するが、一致するのであれば、ステップS80において、Usage Rule#xにおいてMove制御情報に示されるMove許可回数をデクリメントし、ステップS81において、デクリメントされたMove許可回数と、CheckOut制御情報とを含むUsage Rule#xをローカルストレージにセキュアライトする。続いてステップS77では、SDメモリカード100におけるUsage Rule#xのAvailability Flagに“0”を、Content IDに“0”をセキュアライトし、それ以外のUsage Rule#xのフィールド(STI_KEYを含む)に乱数をセキュアライトすることにより、Usage Rule#xをSDメモリカードから削除する。加えて、SDメモリカード100においては、SD_AUDIO.TKMファイル中のTKI#xを無効にし、さらには、SD_AUDIO.PLNファイル中のデフォルトプレイリストから、TKI#xに関連する情報を削除する。また、POB000.POMファイルに対しては、TKI#xにて参照されているPOBファイルの参照カウンタを1減算する。Move時にこのカウンタが0となった場合

は、当該POBファイルを削除する。

【0120】その後、ステップS82において、トラック#xを構成するAOB#x、STKI#xをSDメモリカード100におけるユーザデータ領域から読み出して、ローカルストレージ32におけるユーザデータ領域に記録する。ステップS83においてAOB#xについてのTitle_Key_EntryをSDメモリカード100におけるプロテクト領域からセキュアリードして、ローカルストレージ32におけるプロテクト領域にセキュアライトする。以上で、トラック#xを構成するデータセットは、ローカルストレージ32に格納されたこととなる。

【0121】その後、ステップS78においてライブラリ管理部37は、変数#xがUsage Rule Managerにおけるラストナンバーか否かを判定し、そうでないならステップS79において#xをインクリメントした後、ステップS73に移行する。これらの処理をAOBSA1.URMに含まれる全てのUsage Ruleについて繰り返せば、SDメモリカード100において移動が可能のように設定されている全てのトラックは、SDメモリカード100からローカルストレージ32へと移動することとなる。配信サーバー103からの著作物購入、又は、SDメモリカード100からの著作物の移動により、カスタマーズデバイスにおけるローカルストレージ32には、多くの著作物が蓄積され、ホームライブラリが構築されることとなる。

【0122】トラックのチェックアウトが要求された場合、図39のステップS43がYesとなり、図40のステップS66に移行する。ステップS66では、SDメモリカード100以外の他の記録媒体に記録すべきトラックの選択待ちを行い、選択されれば(選択されたトラックをトラック#xと呼ぶ。)、ステップS100においてライブラリ管理部37は、カスタマーズデバイスに接続されたSDメモリカード100に固有なMedia-IDを読み出す。一方、このSDメモリカード100における空きのContent_IDを探し出して、選択されたトラックにこの空きのContent_IDを割り当て、Media-IDと、Content_IDとの組みをチェックアウト履歴情報として記憶する。その後、ステップS49においてトラック#xに対応するUsage Rule#xのセキュアリードを行う。ステップS50では、Usage Rule#xにおいてCheck-Out制御情報に示されている回数(Check Out回数という)が“0”であるか否かを判定する。Check Out回数が“0”であれば、ステップS51～ステップS57の処理をスキップしてステップS42～ステップS45の処理に移行するが、“0”でなければ、ライブラリ管理部37はステップS51においてトラック#xを構成するデータセット(Usage Ruleを除く)を他の記録媒体に記録する。チェックアウト時において、可搬型記録媒体には、図12に示したようなディレクトリ構成、ファイル構造のうち、SD-Audio Ver1.0規格に規定されたもの、即ち、『AOBxxx.SA1』『POBxxx.SP1』『SD_AUDIO.TKM』『SD_AUDIO.PLN』『POB000.PO

M』、『AOBSA1.KEY』、『POBSP1.KEY』が記録される。これにより、トラックが記録されることとなる。そのためトラック統合、トラック分割といったトラック編集や、順方向、逆方向サーチ再生が可能となる。

【0123】続いてステップS52においてCheck Out回数をデクリメントし、ステップS53では、Check Out回数が“0”であるか、1以上であるか否かを判定する。Check Out回数が“0”であれば、ステップS54において、トラックを“チェックアウト不可能”に設定した後、ステップS55に移行する。Check Out回数が“1”以上であれば、ライブラリ管理部37は、ステップS55において、デクリメントされたCheck Out回数をローカルストレージ32におけるUsage Ruleにセキュアライトする。その後、ステップS56においてUsage RuleにおけるCheck Out回数のベリファイを行い、ステップS57においてUsage RuleにCheck Out回数が正常に書き込まれたか否かを判定する。正常に書き込まれたなら、ステップS42～ステップS45からなるループ処理に移行する。

【0124】操作者からチェックインが要求されたなら、ステップS44がYesとなり、ステップS101において、既にトラックが記録されているSDメモリカードから、SDメモリカードに固有なMedia-IDと、トラックに固有なContent_IDとを読み取る。ステップS102では、読み取られたMedia-IDとContent_IDとの組みと、チェックアウト履歴情報におけるMedia-IDとContent_IDとの組みとを照合し、ステップS103においてSDメモリカード100に記録されているトラックが、過去にチェックアウトされたものと同一であるか否かを判定する。もし両者が一致である場合（過去にチェックアウトされたものと同一である場合）、ステップS58に移行するが、両者が不一致である場合（過去にチェックアウトされたものでない場合）、チェックイン処理を行わずにステップS42～ステップS45の処理に移行する。

【0125】ステップS58では、ローカルストレージ32のプロテクト領域におけるUsage Ruleをセキュアリードして、ライブラリ管理部37はステップS59においてUsage RuleにおけるCheck Out回数が“0”か否かを判定する。Check Out回数が“0”ならば、ステップS60においてトラックを構成するデータセットのうち、Usage Rule以外のものを、チェックインを行うべき記録媒体から読み出し、ローカルストレージ32に蓄積した後、ステップS92に移行する。Check Out回数が“1”以上なら、そのままステップS66に移行する。ステップS92では、トラックを構成するデータセットを他の記録媒体から削除する。ステップS61では、Check Out回数をインクリメントして、ステップS62においてCheck Out回数が最大数Maxか否かを判定する。Check Out回数がMaxなら、ステップS42～ステップS45からなるループ処理に移行し、Check Out回数がMaxでないなら、

ライブラリ管理部37はステップS63においてCheck Out回数をセキュアライトし、ステップS64においてCheck Out回数をベリファイする。ステップS65では、セキュアライトが正常に行われたかの判定を行い、セキュアライトされたCheck Out回数が正常ならば、ステップS42～ステップS45からなるループ処理に移行する。

【0126】以上説明したように本実施形態によれば、KIOSK端末にて記録された著作物の複製物の記録管理がパソコン上で可能となるので、正当な料金を支払って、KIOSK端末から著作物を購入したユーザは、その著作物についてのチェックアウト チェックインを自分が所有するパソコンに行わせることができる。

（第2実施形態）第2実施形態は、著作物の試聴（プレビュー）を行わせるよう、著作物をセキュアに格納したSDメモリカード100についての改良に関する。図42は、第2実施形態に係るプロテクト領域と、ユーザデータ領域のディレクトリ構成を示す図である。本図と、図12に示したディレクトリ構成とを比較して新規なのは、プロテクト領域及びユーザデータ領域におけるSD_Audioディレクトリのサブディレクトリとして、SD_ADPRVディレクトリが設けられている点である。ユーザデータ領域におけるSD_ADPRVディレクトリには、プレビュー用に設けられた『SD_ADPRV.PLM』、『SD_ADPRV.TKM』、『P_AOBxxx.SA1』、『P_POBxxx.JPG/SP1』が配置されている。『SD_ADPRV.PLM』、『SD_ADPRV.TKM』は、配置されているディレクトリが異なるだけで、そのデータ構造は、SD-Audio規格におけるSD_AUDIO.PLM、SD_AUDIO.TKMと全く同一である。P_AOBxxx.SA1、P_POBxxx.JPG/SP1は、配置されているディレクトリと暗号化に用いられた暗号鍵とが異なるが、SD-Audio規格におけるAOBxxx.SA1、POBxxx.SP1/JPGと同一である。

【0127】プロテクト領域におけるSD_ADPRVディレクトリには、『P_AOBSA1.KEY』、『P_POBSP1.KEY』が配置されている。P_AOBSA1.KEYには、複数のExtended Title Key Entryが含まれている。これらのExtended Title Key Entryのデータ構造を図43に示す。本図において、一部のデータ構成はTitle Key Entryと同一であるが、プレビュー用のフィールドが新たに追加されている点異なる。図43のExtended Title Key Entryのフォーマットにおいて、プレビュー用のフィールドには、『Trigger Bit』、『Preview Counter』、『Preview Threshold』、『Check=Valueフィールド』が存在する。

【0128】『Trigger Bit』は、Usage RuleにおけるTrigger Bitと同様の趣旨で設けられたフラグであり、“0”に設定されれば、Preview Counter及びPreview Thresholdの組みを参照することにより、プレビューの可否を判定して良い旨を示し、“1”に設定されれば、Preview Counter及びPreview Thresholdの組みだけでなく、他の情報を参照することにより、プレビューの可否を判定す

べき旨を示す。

【0129】『Preview Counter』は、1～255の範囲でプレビューの許可回数を示すフィールドであり、図11に示したDefault OfferのDRMにおけるPlayback Counterに基づき設定される。『Preview Threshold』は、著作物が何秒再生されれば、プレビュー回数を1回とカウントするかを指示するフィールドであり、図11に示したDefault OfferのDRMにおけるPlayback Timeに基づき設定される。

【0130】『Check-Valueフィールド』には、チェック用の文字列パターンが記述される。C_CBCモードによるExtended Title Key Entryの復号が正常に得られた場合、この機器は、本フィールドから文字列パターンを正常に得ることができるが、Extended Title Key Entryの一部が暗号化された状態のまま改竄された場合、このフィールドから文字列パターンを得ることができない。その理由は以下の通りである。

【0131】C_CBCモードによる復号は、7バイトのMedia-ID及び部分鍵を用いることにより、8バイトを一単位として行われる。ここでもし、悪意をもったユーザが、暗号化されたままPreview Counter、Preview Thresholdを全く別の値に改竄したとする。そうすると、このPreview Counter、Preview Thresholdを含む8バイトブロックを部分鍵を用いて得られる部分鍵は、予定されていたものと大きく異なるものが得られる。そうした部分鍵を用いて、後段のブロックを復号してゆくと、最後に文字パターンを含むブロックを復号することにより得られた演算結果は、上述した文字パターンと大きくかけはなれたものとなる。このように、文字パターンは、暗号化されたPreview Threshold、Preview Counterが正常な状態である限り、正常な文字列パターンが復号されることとなるが、Preview Threshold、Preview Counterが改竄されていれば、改竄のAOBファイルを受けて、Check-Valueフィールドにおける文字列パターンは、全くおかしいものとなる。こうした文字列パターンの性質を利用して、Preview Threshold、Preview Counterに対する改竄の有無をチェックすることができる。

【0132】続いて、第2実施形態におけるSD-AUDIOプレーヤ122～SD-AUDIOプレーヤ124の処理について説明する。図43に示したExtended Title Key Entryを用いて、著作物のプレビューを行う場合、SD-AUDIOプレーヤ122～SD-AUDIOプレーヤ124に含まれる制御部64がどのような処理を行うかは、図44のフローチャートに示されている。以降図44を参照しながら、第2実施形態における制御部64の処理について説明する。

【0133】制御部64は、ステップS81においてSDメモリーカード100がカードコネクタ34に接続されたかどうかを判定し、ステップS82においてSDメモリーカード100のSD_ADPRVディレクトリにおけるトラックを一覧表示する。ステップS83においてプレビューすべ

きトラックの選択待ちを行う。ここで操作者により選択されたトラックをトラック#xとするとステップS84においてトラック#xについてのExtended Title Key Entry #xをプロテクト領域からセキュアリードする。その後、ステップS85において制御部64は、Trigger Bit#xをチェックする。Trigger Bitが“1”であれば、ステップS86～ステップS97の処理は行わず、処理は終了する。Trigger Bitが“0”であれば、ステップS86において、制御部64は、Extended Title Key Entry#xに対して、C_CBCモードの復号を行うことにより、文字列パターンを得る。ステップS87において文字列パターンは正常なものかどうかを判定する。異常であれば、処理を終了するが、正常ならば、ステップS88において制御部64は、Preview Counterが“0”であるかどうかを判定する。Preview Counterが“0”であれば処理を終了するが、そうでなければ、制御部64は、ステップS89において、Extended Title Key Entry#xにおけるTitle KeyをSDメモリーカード100におけるデスクランブラ61に設定する。その後制御部64は、ステップS90においてトラック#xを再生する。制御部64は、ステップS91においてPreview Threshold#xに示された時間だけ再生時間が経過するのを待ち、経過すれば、ステップS92においてPreview Counterをデクリメントする。その後、ステップS93においてPreview Counterが1以上であるか0であるかを判定する。1以上であればステップS94においてPreview Counterをセキュアライトし、その後、ステップS95においてPreview Counterをベリファイする。Preview Counterが“0”であれば、ステップS96においてTitle Key Entryを削除し、ステップS97においてAvailability Flagに“0”を設定する。

【0134】以上のように本実施形態によれば、Preview Counter、Preview Thresholdは、プロテクト領域に記録されており、改竄は非常に困難となるので、著作物についての著作権を正当に保護しながら、著作物の試聴を操作者に行わせることができる。以上、2つの実施形態に示される配信システムを運用した場合、著作物の販売は、音楽会社が運営する配信サーバー103と、自動販売機、携帯電話機、STBとの間で行われるので、著作物の販売にあたっての流通コストや在庫管理が大きく軽減されることとなる。また、パソコンを所持していないユーザであっても、販売店まで足を運ばずに、携帯電話機やSTBを介して著作物を購入することができ、価格の低下が期待できるなどメリットも大きい。既存の流通経路を大きく改良できる。これらの点において、本発明に係る配信システム、受信装置、半導体メモリーカードは高い産業上の利用可能性を有する。

【0135】尚、これらの実施形態は、現状において最善の効果が期待できる形態を記述したものであって、上記実施の形態に限定されるものではない。具体的には、下記のような変更実施が可能である。

(a)第1、第2実施形態における、SDメモリカードは、ユーザデータ領域と、プロテクト領域を備えたが、これに限定されるものではなく、すべてプロテクト領域として実現してもよい。記録媒体としてSDメモリカード100を使用したか、このような半導体メモリに限定されるものではなく、プロテクト領域を備えていれば、光ディスク、HD等に置き換えることが可能である。

【0136】(b)第1、第2実施形態では、1個の著作物はパッケージに対応し、音楽アルバム等、著作物の集合体は、タイトルに対応したが、著作物の集合体を1個のパッケージにて送信してもよい。

(c)トラックのプレビューを行うための条件として、日付による制限(ある期日までは試聴可能)、試聴日数による制限(特定の時間、日数の間は試聴可能)、試聴範囲の制限(トラックの特定の部分のみ試聴可能)、という条件を採用したり、あるいは、これらの組み合わせを採用してもよい。

【0137】(d)第1、第2実施形態では、記録再生の対象となるデータを音楽データ、および静止画に限定して説明を行ったが、これに限定されるものではない。記録再生の対象となるデータは任意のデジタルデータであり得る。例えば、記録再生の対象となるデータは、動画、テキストデータ、または、これらを組み合わせることによって得られるデータであってもよい。

【0138】(e)第1実施形態においてデジタルターミナルは、DRM中のMove制御情報を参照し、DRMに忠実に、Usage RuleのMove制御情報に設定していたが、デジタルターミナルは、他の情報を参照して、他の基準にてMove制御情報を設定してもよい。例えば、著作物のヒットチャートにおけるランクや、著作物が新譜であるか否か、著作物の売り上げ高等の情報を勘案して、Move制御情報を設定してもよい。

【0139】(f)ローカルストレージに書き込まれた暗号化データ、ブレンデータ、暗号鍵、権利証をローカルストレージから読み出し、権利証において移動許可回数に示される回数が0(ゼロ)であるか、1以上であるかを判定を行なって、回数が1以上なら、これらをSDメモリカード100に再度記録してもよい。

(g)第1実施形態では、SDメモリカード100に移動許可回数が“1”又は“0”に設定されることを想定していたが、これ以上の移動許可回数を設定してよいことはいまでもない。配信サーバー103により“移動許可回数=6回”と移動制御情報が設定された場合には、移動制御情報に示される移動許可回数は図45のように更新されながら、権利証は各記録媒体間を移動してゆくこととなる。

【0140】

【発明の効果】以上説明したように、本発明に係る配信システムは、第1受信装置、第2受信装置を含み、前記第1受信装置は、コンテンツと、記録媒体に対する当該

コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第1受信手段と、前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージルール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備え、前記第2受信装置は、前記データセットをネットワークを介して配信サーバから受信して、保持する第2受信手段と、前記配布媒体から許可情報を読み出し、読み出された許可情報に、データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、第2受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備えており、1つの機器から2つの受信装置へとコンテンツとユーセージルールとの組みを移動させるので、第1受信装置(上述の例でいえばKIOSK端末)にて半導体メモリカードに記録されたコンテンツとユーセージルールとの組みの記録管理を第2受信装置(上述の例でいえばパソコン)に行わせることができる。KIOSK端末にて記録された著作物の複製物の記録管理がパソコン上で可能となるので、正当な料金を支払って、KIOSK端末から著作物を購入したユーザは、その著作物についてのチェックアウト チェックインを自分が所有するパソコンに行わせることができる。

【0141】ここで前記チェックアウト手段は、前記記録媒体と接続する接続手段を有していて、当該接続手段に接続された記録媒体に未だコンテンツの複製物が記録されておらず、前記第2受信手段、又は、前記データセット移動手段に保持されている管理情報が、1以上の残り回数を示している場合、データセット移動手段が保持しているデータセットにおけるコンテンツの複製物を記録媒体に記録するものであり、前記第2受信装置は更に、接続手段に接続された記録媒体に既にコンテンツの複製物が記録されている場合、接続手段に接続された記録媒体に記録されているコンテンツの複製物を削除するチェックイン手段と、記録媒体に複製物が記録されれば、チェックアウトの残り回数をデクリメントするよう第2受信手段と、又は、データセット移動手段に保持されている管理情報を更新し、記録媒体におけるコンテンツの複製物が削除されればチェックアウトの残り回数をインクリメントするよう管理情報を更新する更新手段とを備えていてもよい。

【0142】この配信システムによれば、第2受信装置によるチェックアウトは、管理情報に示される回数だけ可能なので、著作権者が定めた限度以上のチェックアウト

トが行われることはない。これにより、著作権者の利益が不当に害されることはない。ここで前記チェックアウト手段は、保持しているコンテンツに、固有の識別子を割り当てて、記録媒体に記録する割当部と、接続手段に接続された記録媒体に固有な識別子を記録媒体から読み出し、これと、割当部により割り当てられたコンテンツの識別子との組みを記憶する記憶部とを備え、チェックイン手段は既にコンテンツの複製物が記録されている記録媒体が接続手段に接続されたなら、当該記録媒体に固有な識別子と、コンテンツに固有な識別子との組みを読み取る読取部と、読取部により読み取られた識別子の組みと、記憶部が記憶している識別子の組みとを比較することにより、接続手段に接続された記録媒体に記録されている複製物が、過去に自装置が記録したものと同一であるか否かを判定する比較部と、過去に自装置が記録したものと同一である場合、接続手段に接続された記録媒体に記録されている複製物を読み出して保持し、その後、記録媒体から複製物を削除する保持部とを備えていてもよい。この配信システムによれば、第2受信装置がチェックインを行う場合、記録媒体の識別子及びコンテンツの識別子の組みを照合することにより、過去に自身がチェックアウトしたものの可否かを判定し、過去に自身がチェックアウトした複製物のみをチェックインするので、『他の機器がチェックアウトしたコンテンツをチェックインしない』という原則が、ないがしろにされることはない。

【図面の簡単な説明】

【図1】著作物のデータ構造を示す図である。

【図2】(a) 暗号鍵、権利証抜きで著作物が記録媒体に記録された態様(1)を示す図である。

(b) 権利証抜きで著作物が記録媒体に記録された態様(2)を示す図である。

(c) 権利証を含んだ状態で著作物が記録媒体に記録された態様(3)を示す図である。

【図3】(a) SDメモ리카ードの外観形状を示す図である。

(b) SDメモ리카ード100の階層構造を示す図である。

(c) SDメモ리카ード100における物理層の構成を示す図である。

【図4】(a) プロテクト領域に暗号鍵のみが格納された状態で非対応機器がSDメモ리카ード100に接続された場合を表す図である。

(b) プロテクト領域に暗号鍵のみが格納された状態で対応機器がSDメモ리카ード100と接続された場合を表す図である。

(c) プロテクト領域に権利証及び暗号鍵が格納された状態で対応機器が接続され、権利証が、移動を許可する旨の移動制御情報を含んでいる場合を表す図である。

(d) プロテクト領域に権利証及び暗号鍵が格納された

状態で対応機器が接続され、権利証に含まれる移動許可回数が0回の場合を示す図である。

【図5】駅構内、店頭にKIOSK端末が設置されている様子を示す図である。

【図6】(a) 携帯電話機タイプのデジタルターミナル109により、著作物を構成する暗号化データ、プレーンデータ、暗号鍵、権利証がSDメモ리카ード100に書き込まれる様子を示す図である。

(b) STBタイプのデジタルターミナル110により、著作物を構成する暗号化データ、プレーンデータ、暗号鍵、権利証がSDメモ리카ード100に書き込まれる様子を示す図である。

【図7】(a) 様々なタイプのカスタマーズデバイスを示す図である。

(b) 様々なタイプのSD-AUDIOプレーヤを示す図である。

【図8】(a) ネットワークに接続された配信サーバー103と、複数のユーザが所有するカスタマーズデバイス(パソコン111~116)とを示す図である。

(b) (c) 3回という範囲でカスタマーズデバイス111がチェックアウト チェックインを行う様子を示す図である。

【図9】本実施形態に係る配信システムに含まれる配信サーバと、複数の機器と、再生装置とを示す図である。

【図10】流通時における著作物データのタイトル及びパッケージのデータ構造を示した図である。

【図11】Default Offerのデータ構造を階層的に示す図である。

【図12】著作物のデータセットを記録するために形成されるファイル、ディレクトリを示す図である。

【図13】AOBファイルのデータ構成を階層的に示す図である。

【図14】AOBファイルに収録されている各AOB、AOB_BLOCKが連続して再生されることにより、どのような再生内容が再生されるかを示す。

【図15】図14に示したタイトル(音楽アルバム)を格納した8つのAOBファイルを示す図である。

【図16】(a) Track Managerの構成を段階的に詳細化した図である。

(b) TKGIの詳細構成を示す図である。

【図17】TKIと、図14に示したAOBファイル及びAOBとの相互関係を示す図である。

【図18】(a) (b) 2つのトラックを1つに統合する場合にTKIがどのように設定されるかを示す図である。

【図19】(a) (b) 1つのトラックを2つのトラックに分割する場合を想定した図である。

【図20】AOB_ELEMENT#1~#4からなるAOBが格納されているクラス007~クラス00Eを示す図である。

【図21】Track Managerに含まれるTKI#2~TKI#4についてのTKI_POB_SRPの設定例を示す図である。

【図22】Default_Playlist情報、TKI、AOBファイルの相互関係を示す図である。

【図23】(a)(b)トラックの順序を入れ替える場合を想定した図である。

【図24】『STKIxxx.SDT』の内部構成を示す図である。

【図25】SD_Audioディレクトリに含まれる3つのAOB#1、AOB#2、AOB#3、2つのPOB001.SP1、POB002.SP1がSD_A DEXTディレクトリに含まれる3つのSTKI001.SDT、STKI002.SDT、STKI003.SDTとどのように対応するかを示す図である。

【図26】AOBSA1.URMの構成を示す図である。

【図27】SD_Audioディレクトリの下にAOBファイルが8つ存在し、これらに対応する暗号鍵がAOBSA1.KEYに8つ収録され、これらに対応するUsage RuleがAOBSA1.URMに8つ収録されている場合、AOBSA1.KEYと、AOBSA1.URMと、AOBファイルとの対応を示す図である。

【図28】(a)(b)AOBSA1.KEY、AOBSA1.URMと、AOBファイルとの対応関係を示す図である。

【図29】Title Key Entryの内部構成を示す図である。

【図30】(a)(b)SDメモ리카ード100におけるユーザデータ領域のオーディオオブジェクトを全てローカルストレージに移動させるケースを想定した図である。

【図31】(a)(b)ユーザデータ領域における8つのオーディオオブジェクトのうち、3つのみを移動させようとする場合、SDメモ리카ード100のユーザデータ領域にどのようなファイルが配置されるかを示す図である。

【図32】図25に示したAOBファイル、POBファイル、STKIファイルがSDメモ리카ード100からローカルストレージへとどのように移動するかを示す図である。

【図33】デジタルターミナルの構成を示す図である。

【図34】(a)カスタマーズデバイスの構成を示す図である。

(b)SD-Audioプレーヤ122～124の内部構成を示す図である。

【図35】デジタルターミナルにおけるセキュア処理部26の内部構成を示す図である。

【図36】カスタマーズデバイスにおけるセキュア処理部38の内部構成を示す図である。

【図37】販売サービス制御部27の処理手順を記載したフローチャートである。

【図38】販売サービス制御部27の処理手順を記載したフローチャートである。

【図39】ライブラリ管理部37の処理手順を記載したフローチャートである。

【図40】ライブラリ管理部37の処理手順を記載したフローチャートである。

【図41】ライブラリ管理部37の処理手順を記載したフローチャートである。

【図42】第2実施形態に係るプロテクト領域と、ユーザデータ領域のディレクトリ構成を示す図である。

【図43】P_AOBSA1.KEYに含まれるExtended Title Key Entryのデータ構造を示す図である。

【図44】プレビューを行う場合のライブラリ管理部37の処理内容を示すフローチャートである。

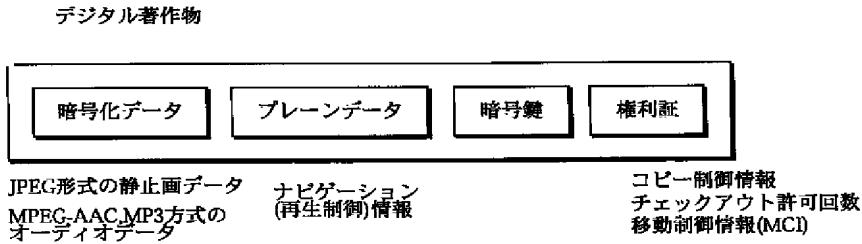
【図45】移動許可回数が6回に設定された場合に、移動許可回数が更新される様子を示す図である。

【符号の説明】

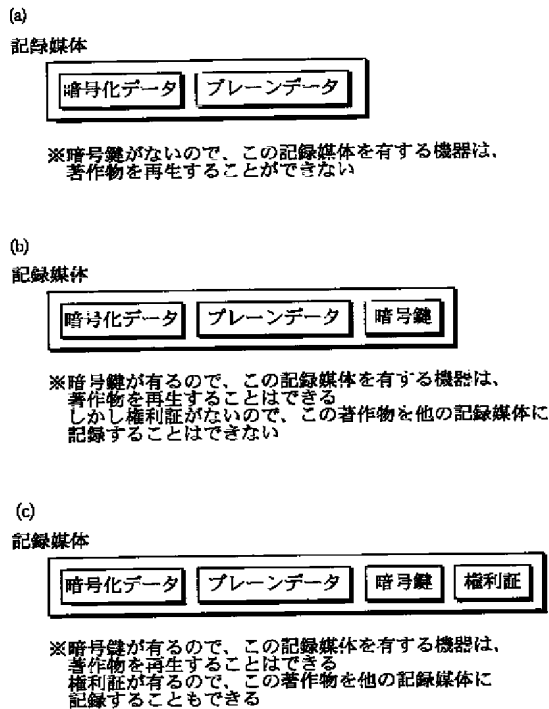
- | | |
|----|----------------|
| 1 | システム領域 |
| 2 | Hidden領域 |
| 3 | プロテクト領域 |
| 4 | AKE処理部 |
| 5 | AKE処理部 |
| 6 | KS復号化部 |
| 7 | KS暗号化部 |
| 8 | ユーザデータ領域 |
| 21 | リリースコンテンツブラウザ部 |
| 22 | タッチパネル |
| 23 | 通信部 |
| 24 | カードコネクタ |
| 25 | 課金部 |
| 26 | セキュア処理部 |
| 27 | 販売サービス制御部 |
| 32 | ローカルストレージ |
| 33 | 通信部 |
| 34 | カードコネクタ |
| 35 | ホームライブラリブラウザ部 |
| 36 | 入力受付部 |
| 37 | ライブラリ管理部 |
| 38 | セキュア処理部 |
| 39 | 再生部 |
| 41 | MKB処理部 |
| 42 | ID処理部 |
| 43 | AKE処理部 |
| 44 | Kmu暗号化部 |
| 45 | STI暗号化部 |
| 46 | Ks暗号化部 |
| 51 | MKB処理部 |
| 52 | ID処理部 |
| 53 | AKE処理部 |
| 54 | Ks復号化部 |
| 55 | Kmu復号化部 |
| 56 | STI復号化部 |
| 60 | カードコネクタ |
| 61 | デスクランブラ |
| 62 | AACデコーダ |
| 63 | A/Dコンバータ |

100	SDメモリーカード	109	携帯電話機
101	プロテクトスイッチ	110	STB
103	配信サーバ	111~121	カスタマーズデバイス
104~108	KIOSK端末	122~124	SD-Audioプレーヤ

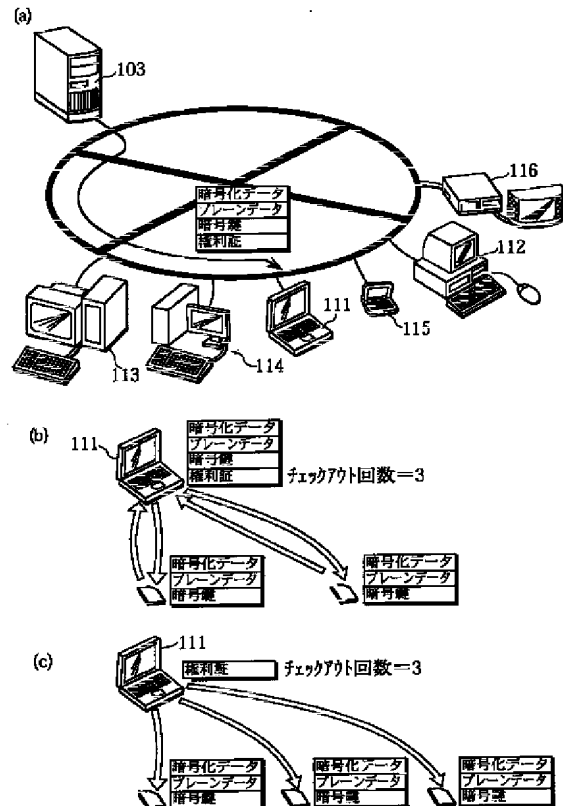
【図1】



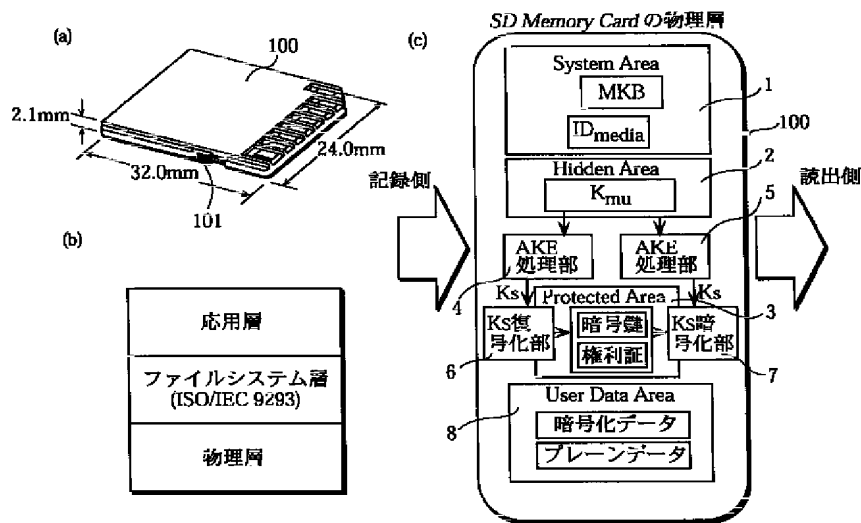
【図2】



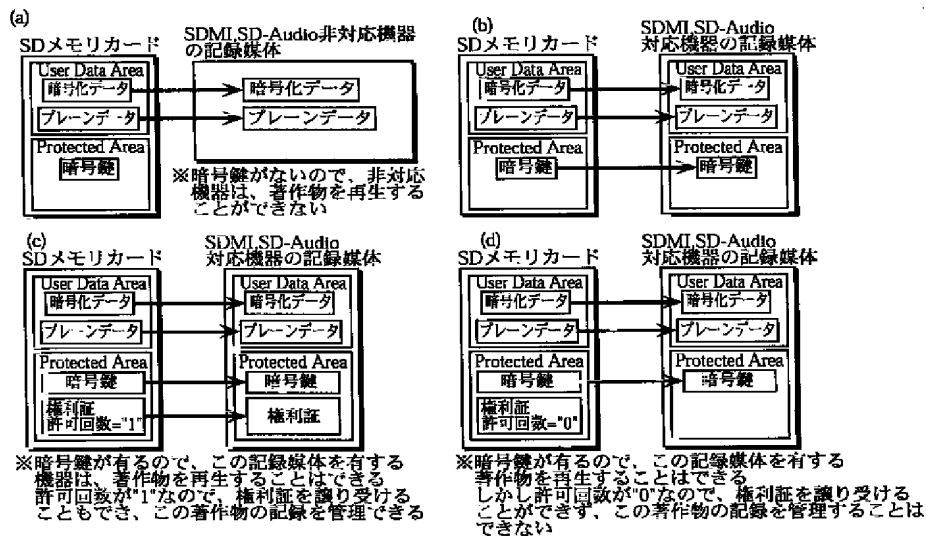
【図8】



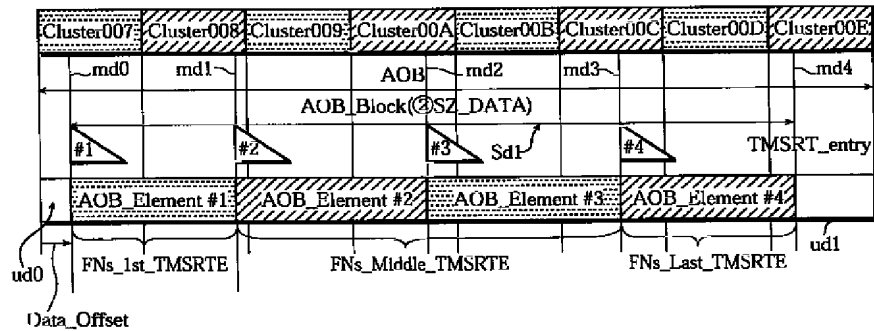
【図3】



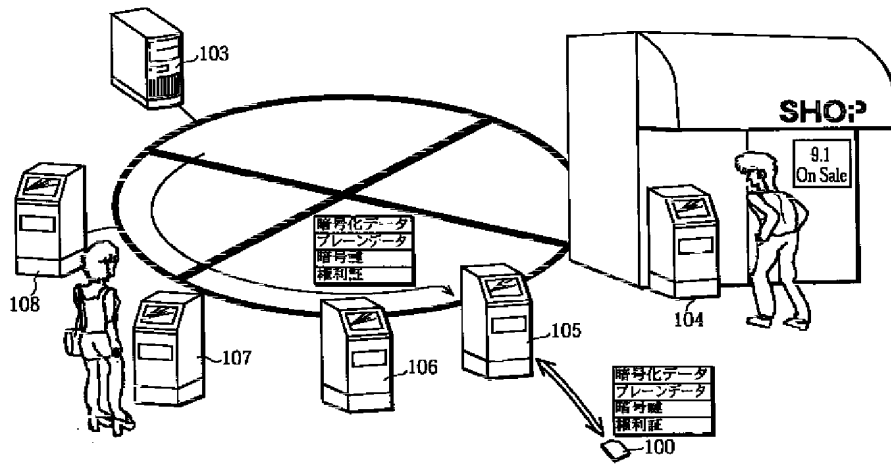
【図4】



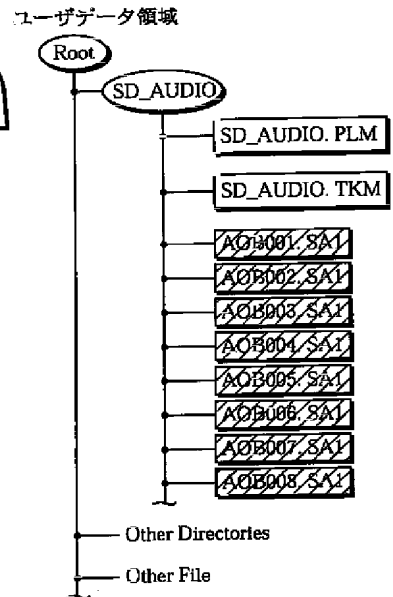
【図20】



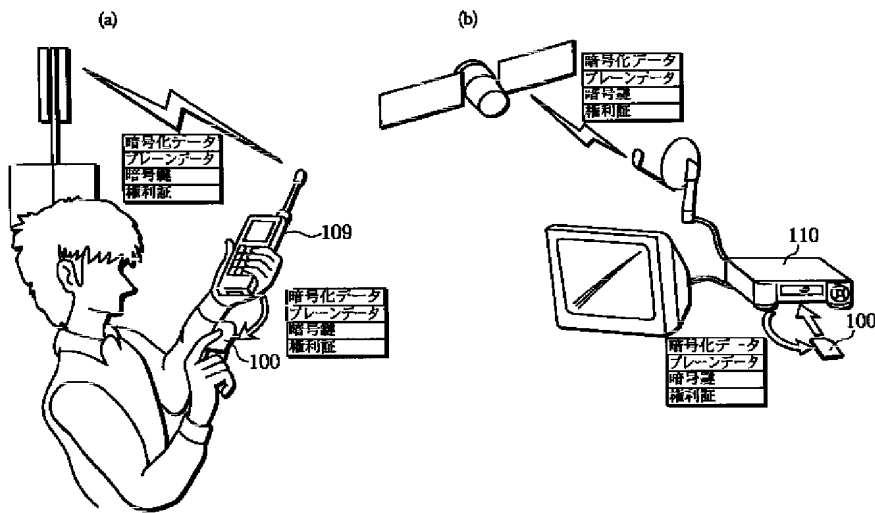
【図5】



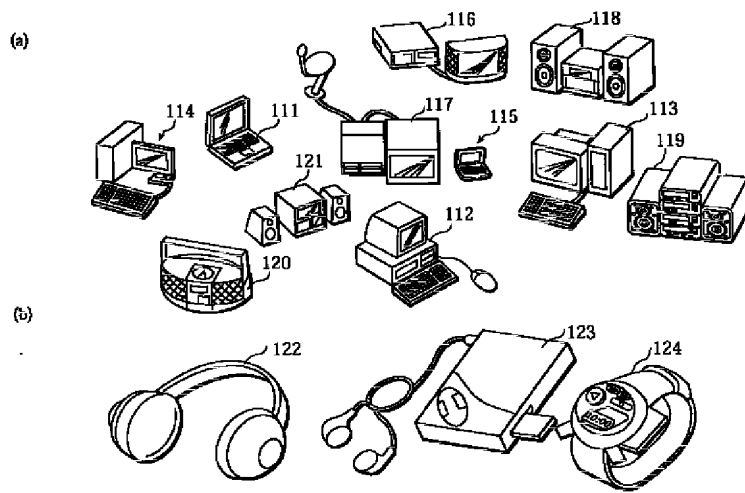
【図15】



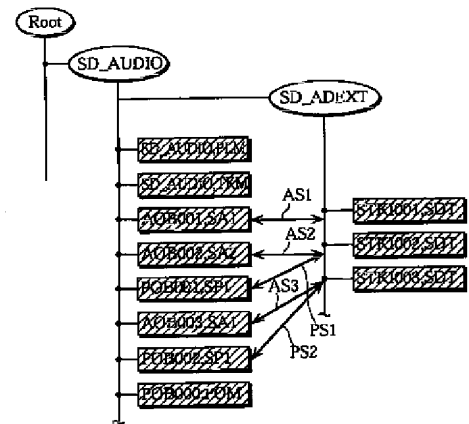
【図6】



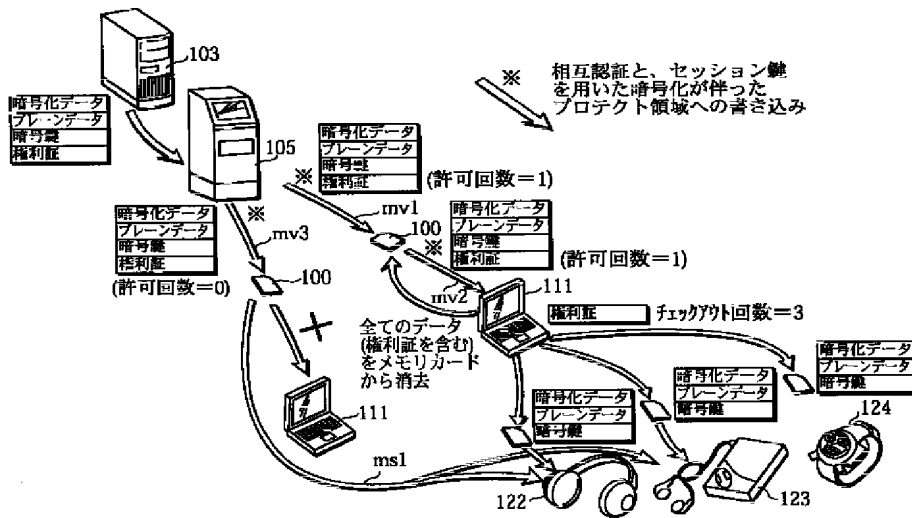
【図7】



【図25】



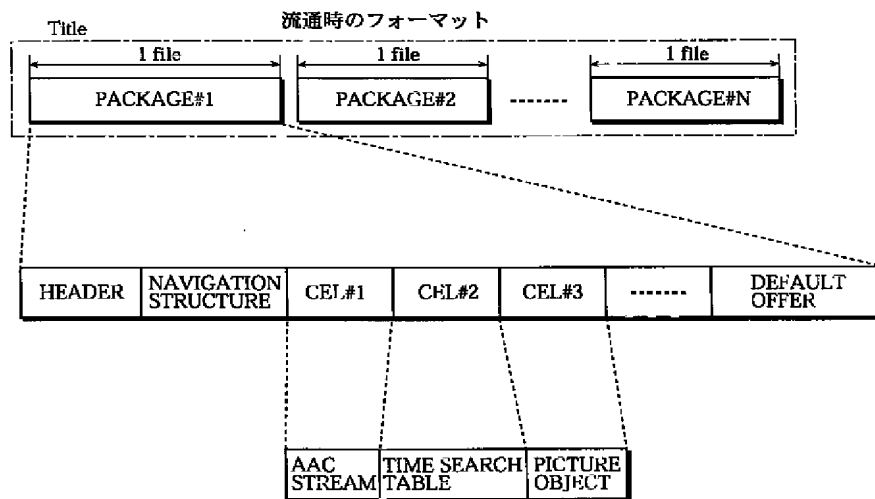
【図9】



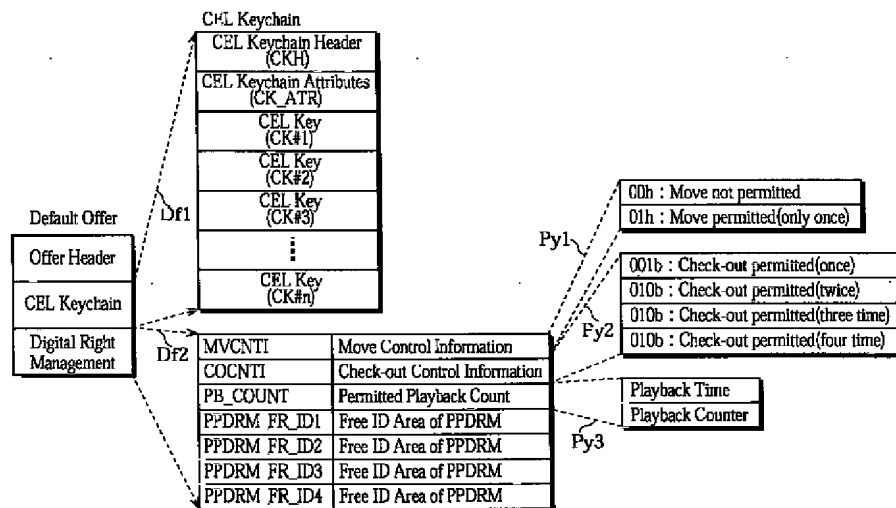
【図29】

AOBSA1.KEY		Title Key Entry
KEY		
Availability flag		
Content ID		

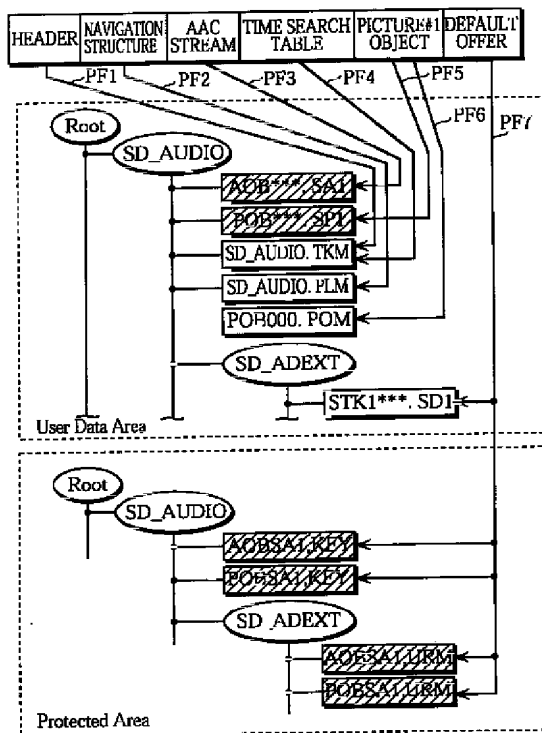
【図10】



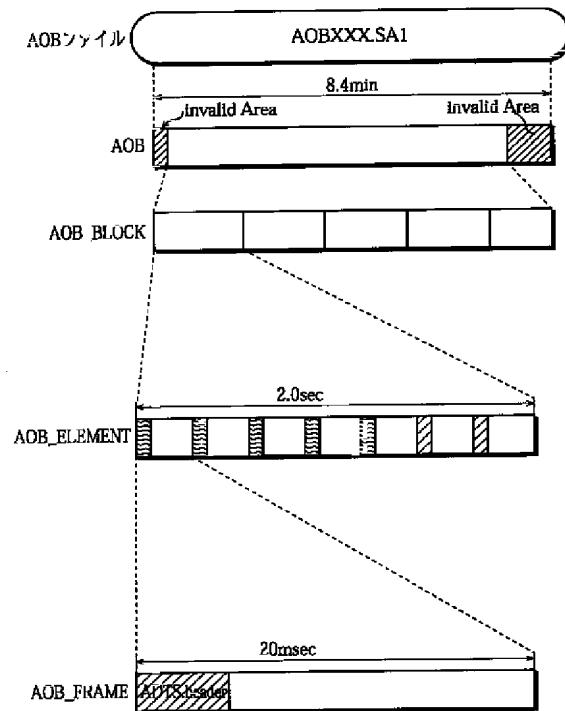
【図11】



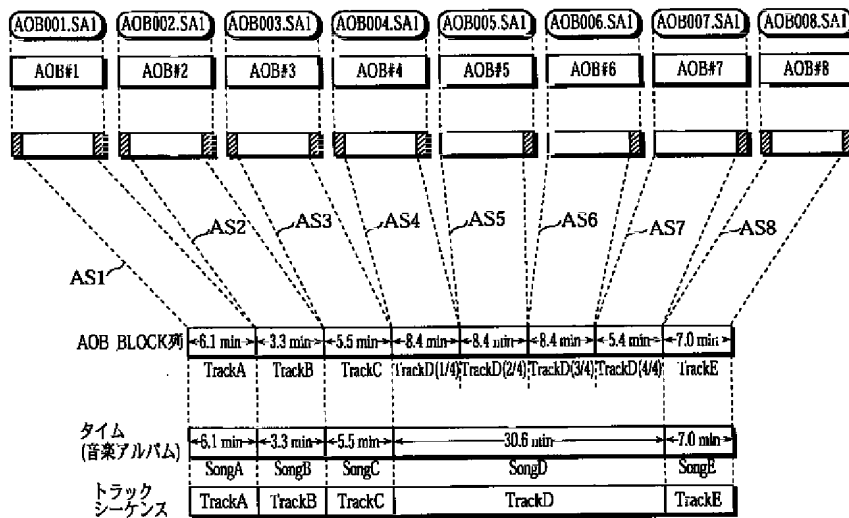
【図12】



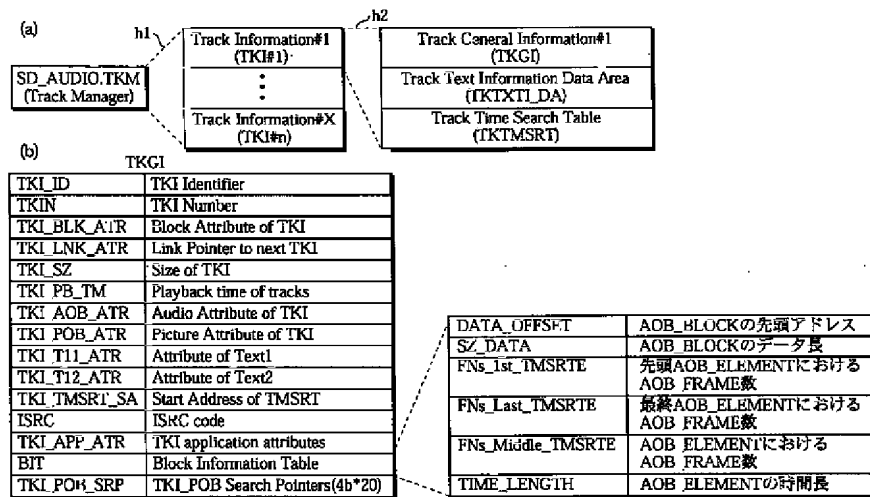
【図13】



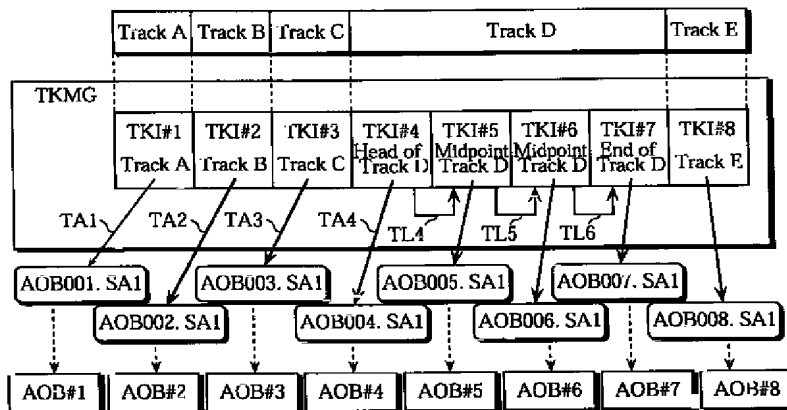
【図14】



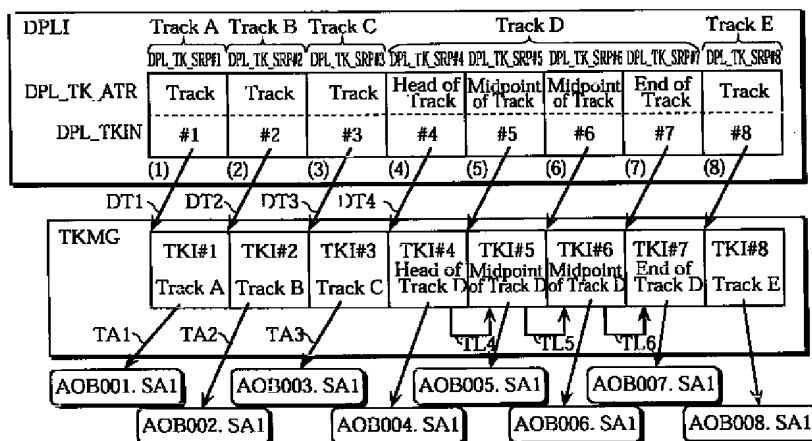
【図16】



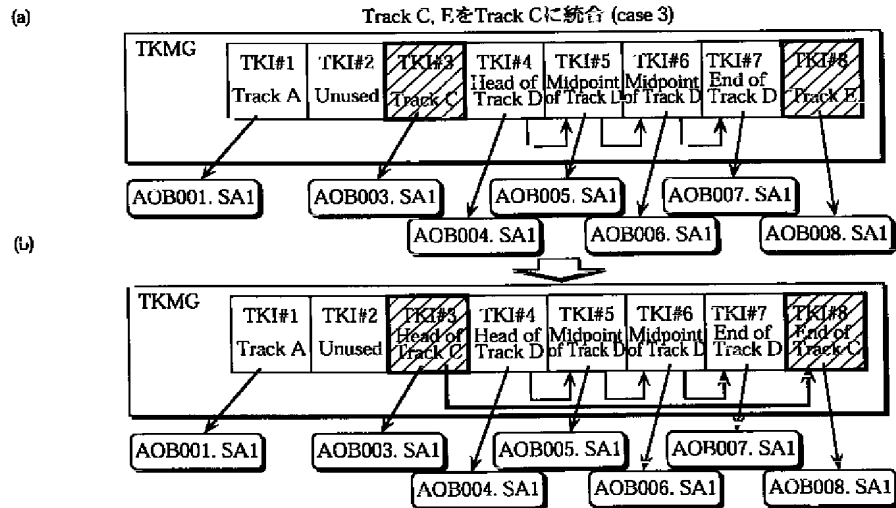
【図17】



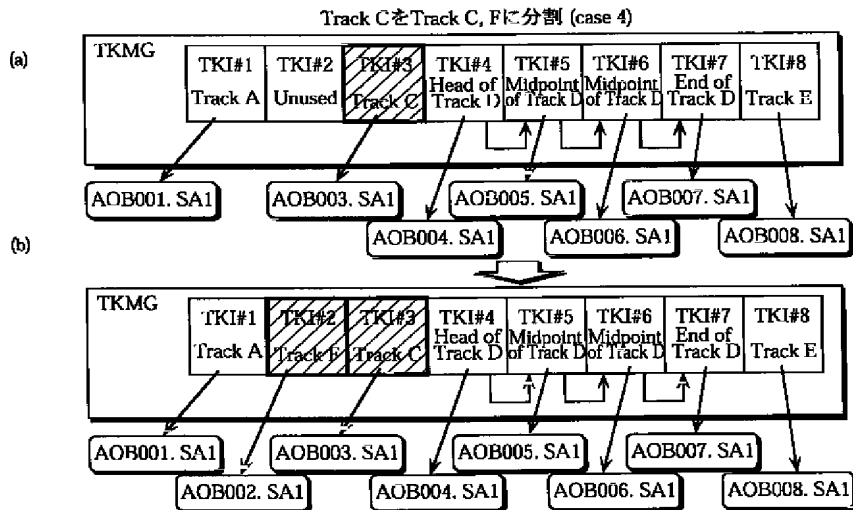
【図22】



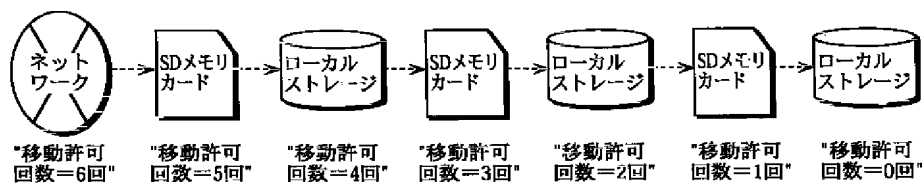
【図18】



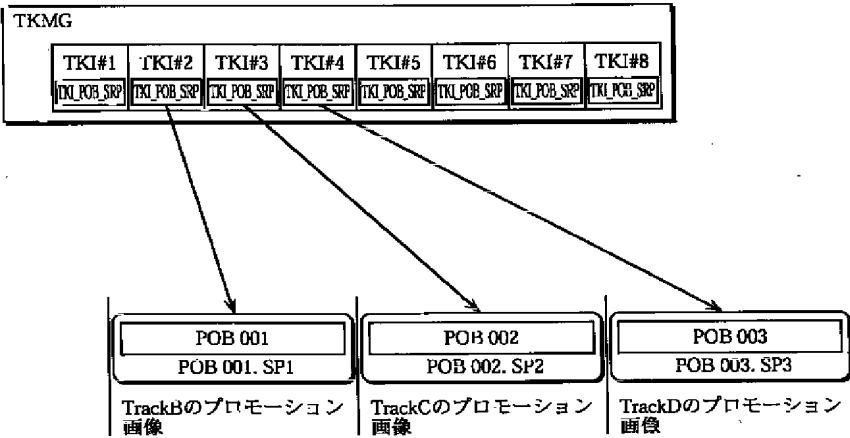
【図19】



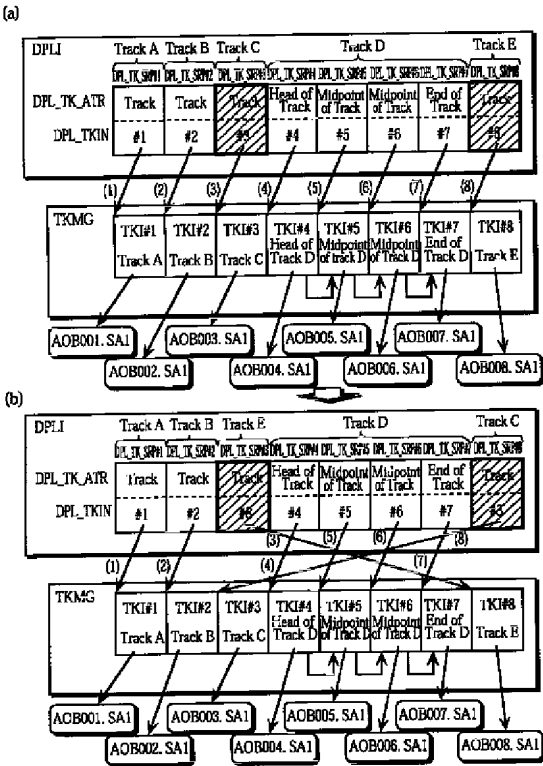
【図45】



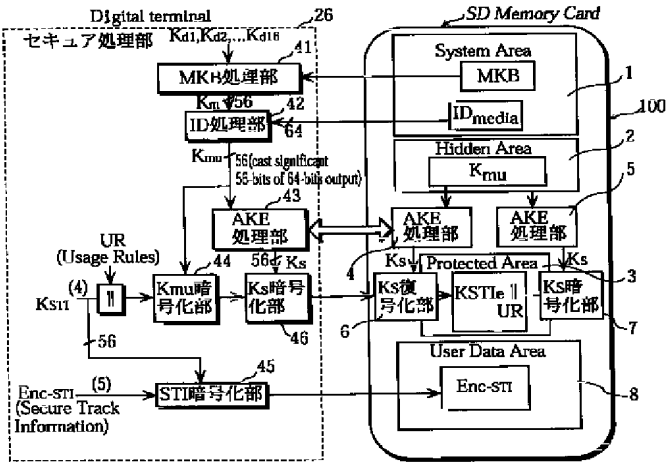
【図21】



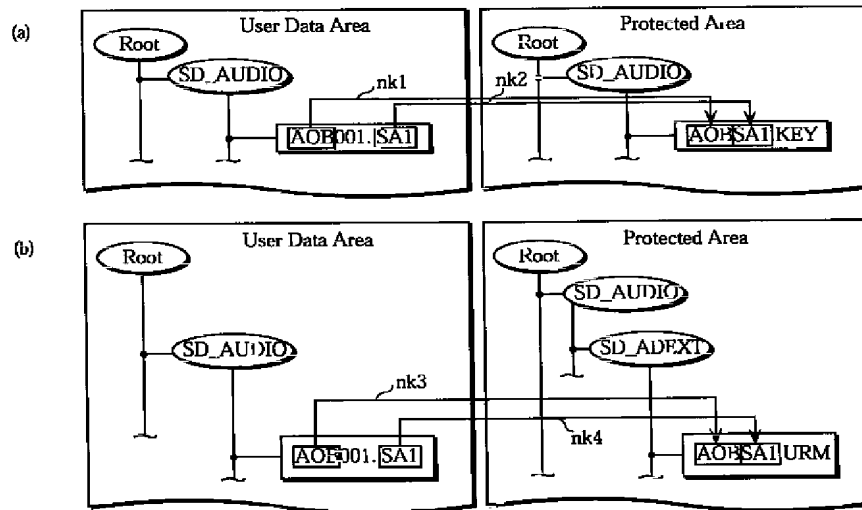
【図23】



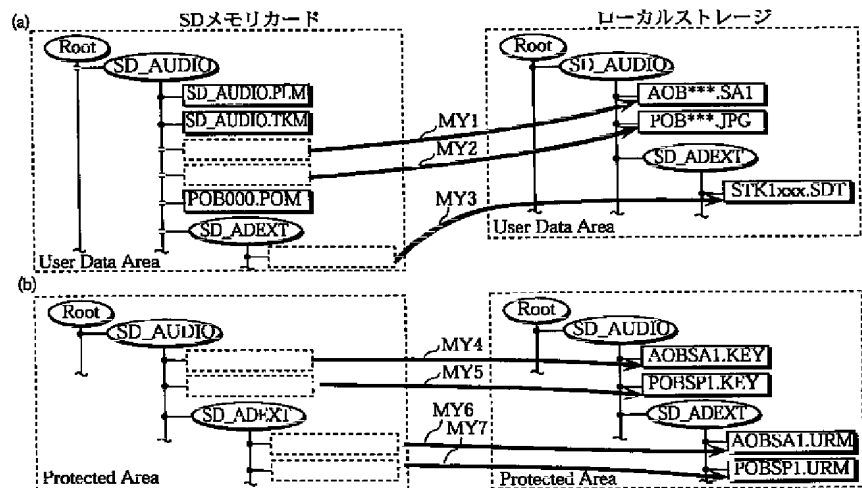
【図35】



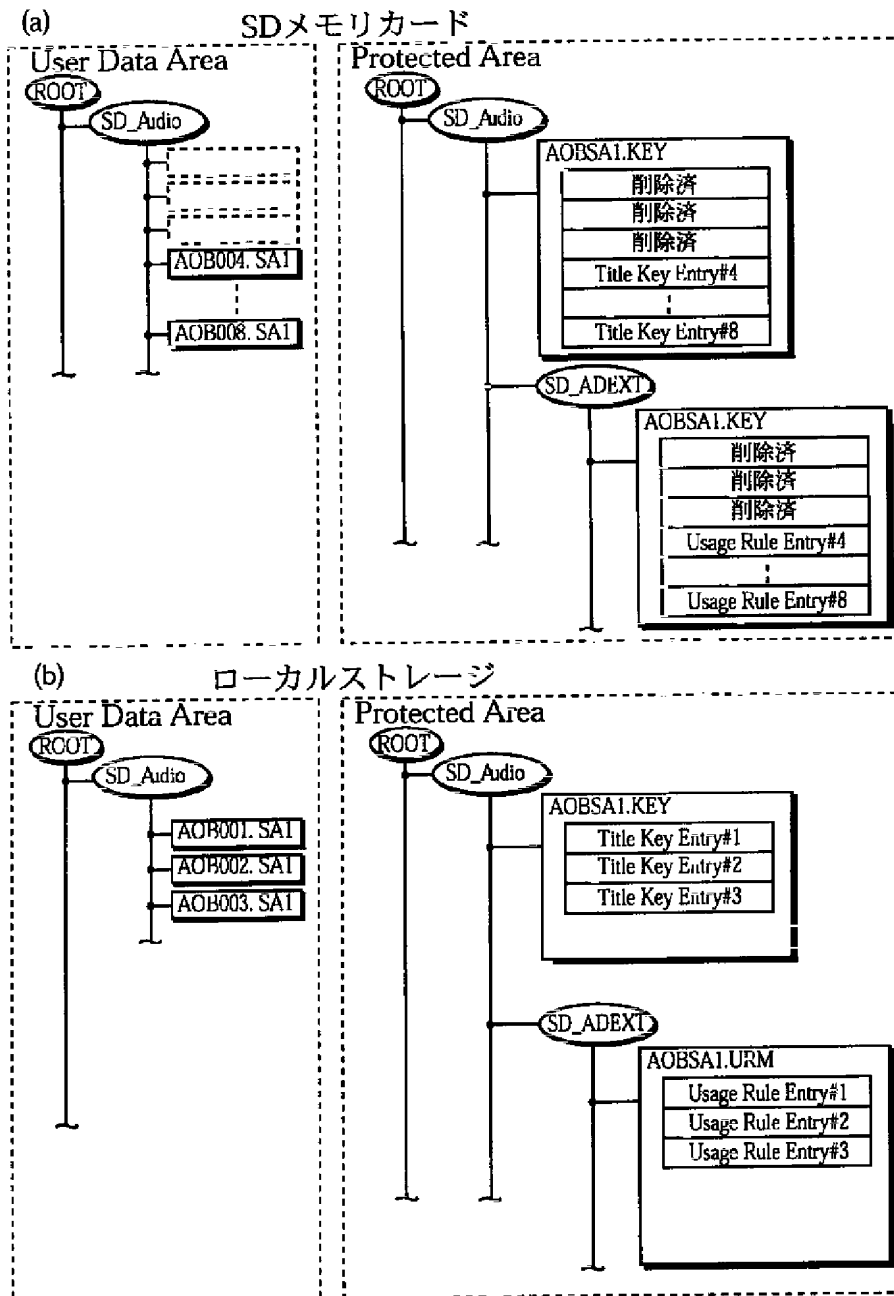
【図28】



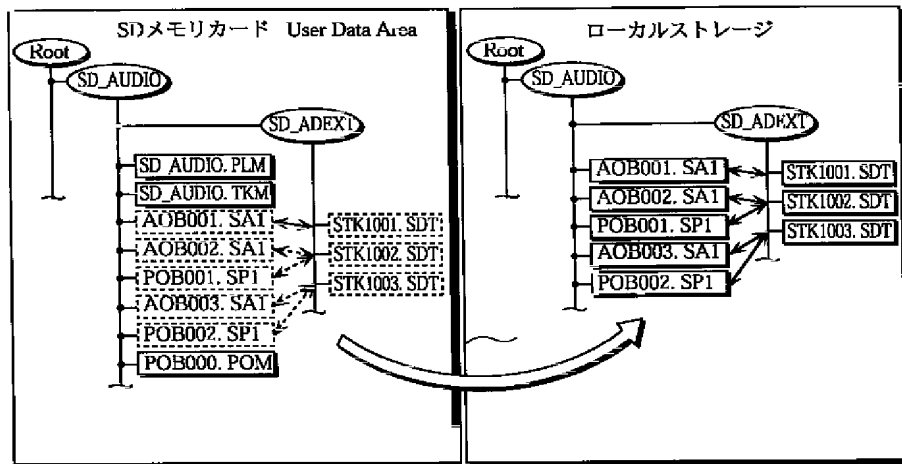
【図30】



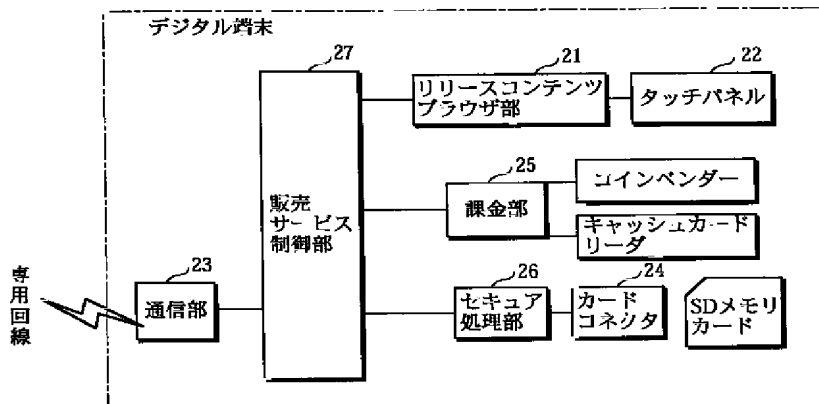
【図31】



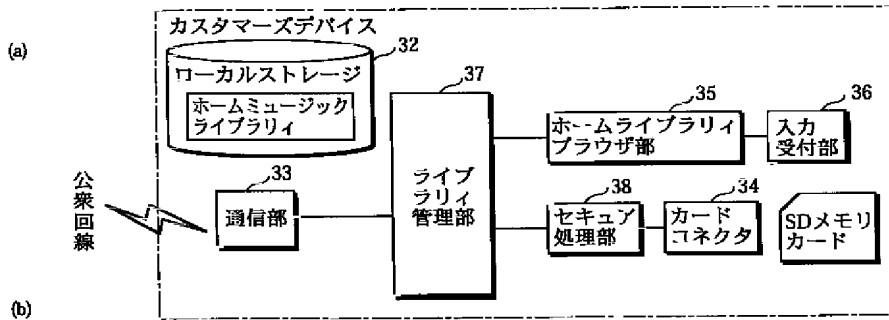
【図32】



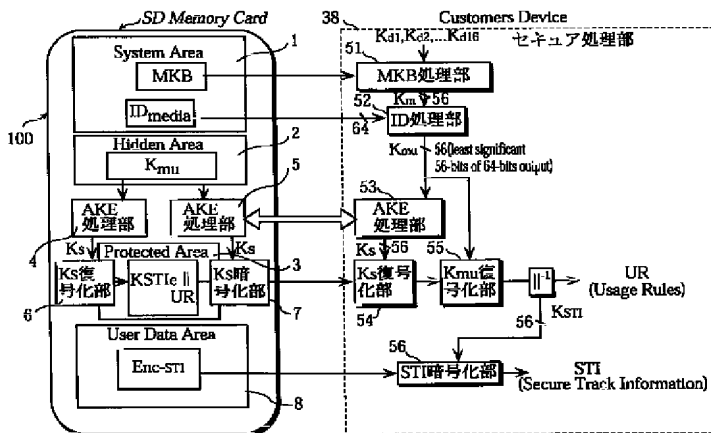
【図33】



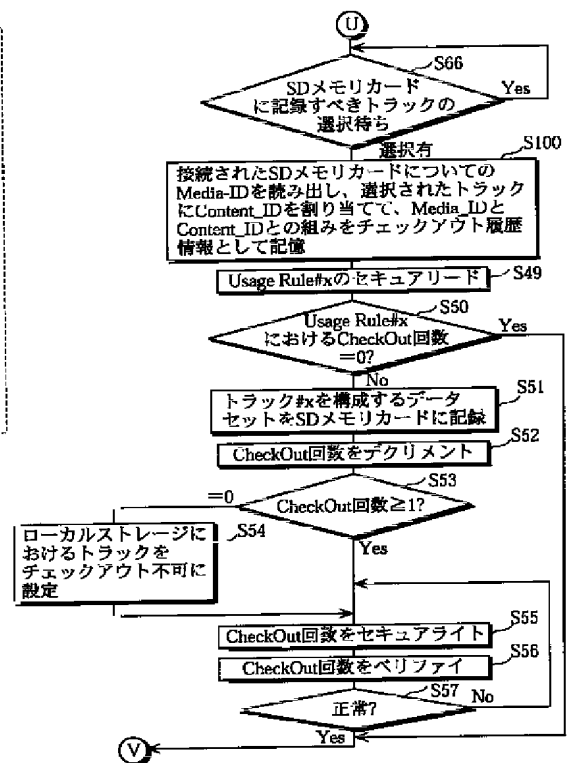
【図34】



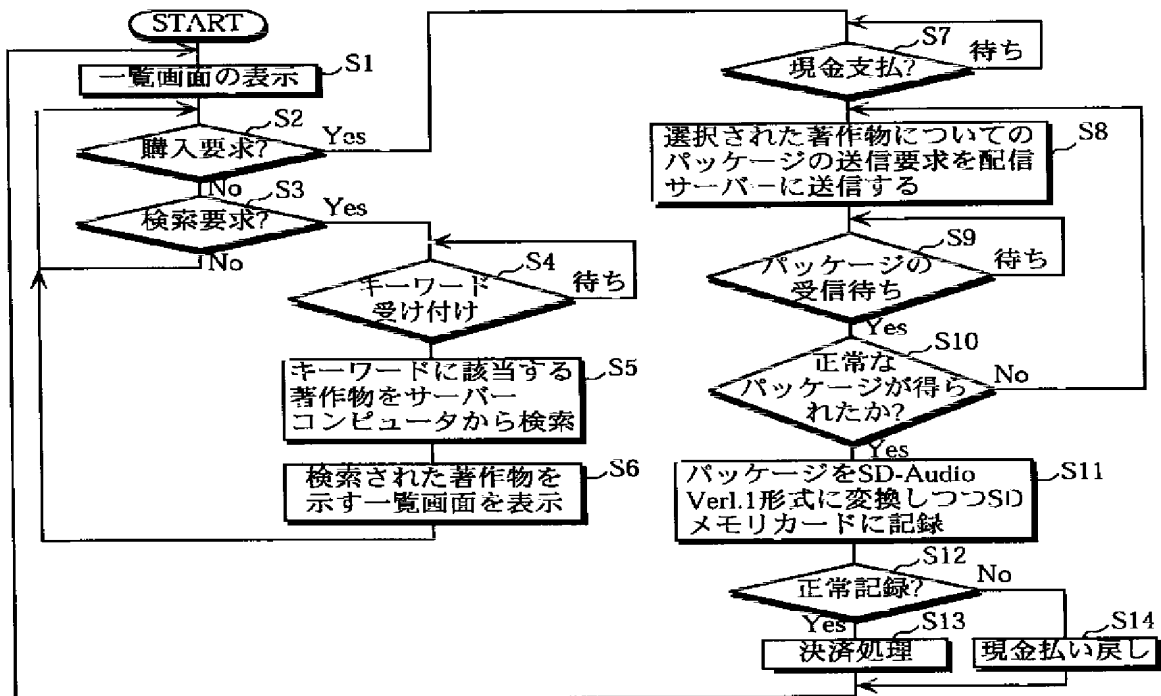
【図36】



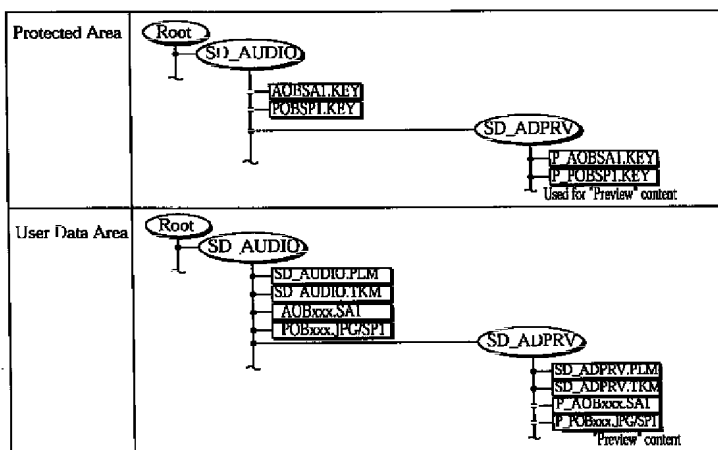
【図40】



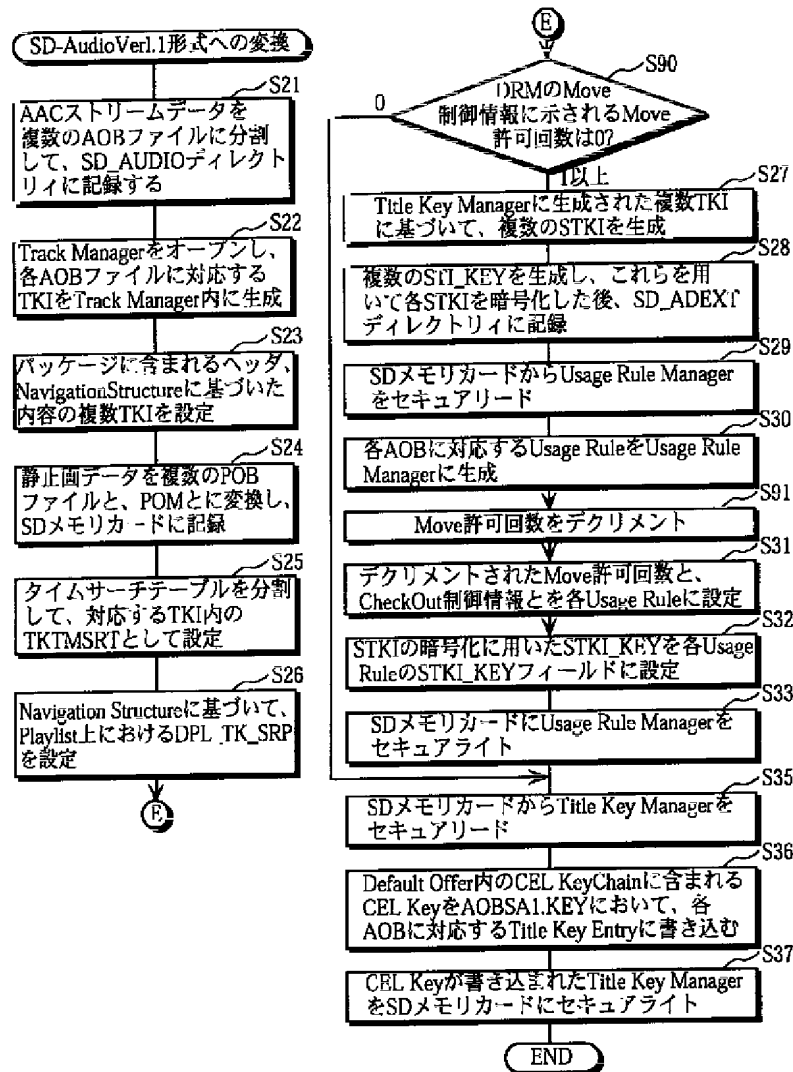
【図37】



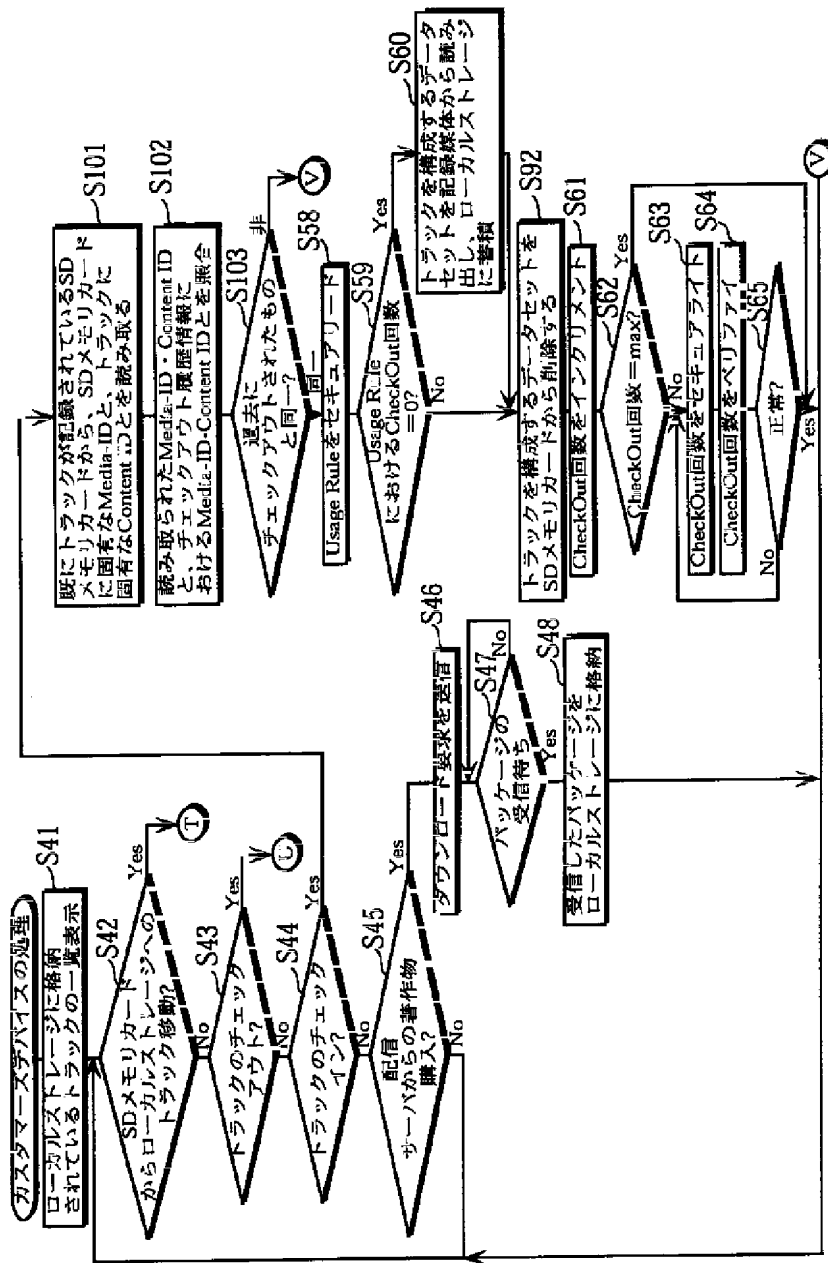
【図42】



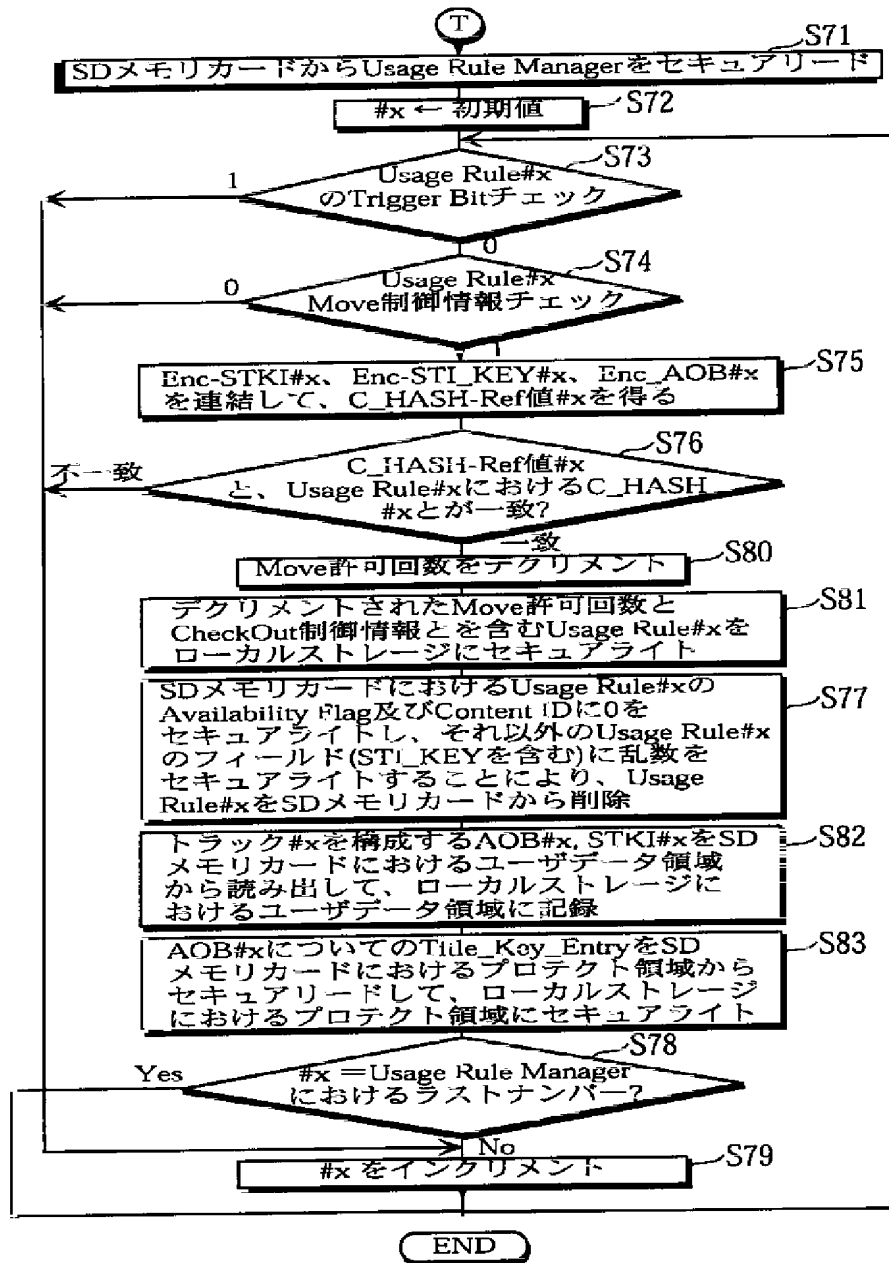
【図38】



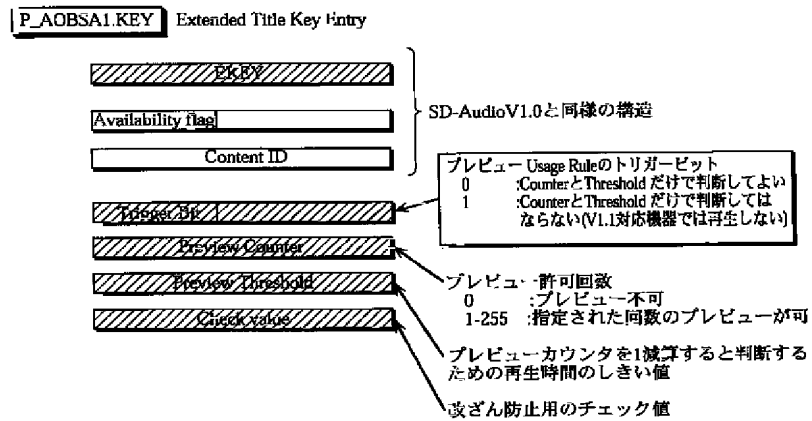
【例 39】



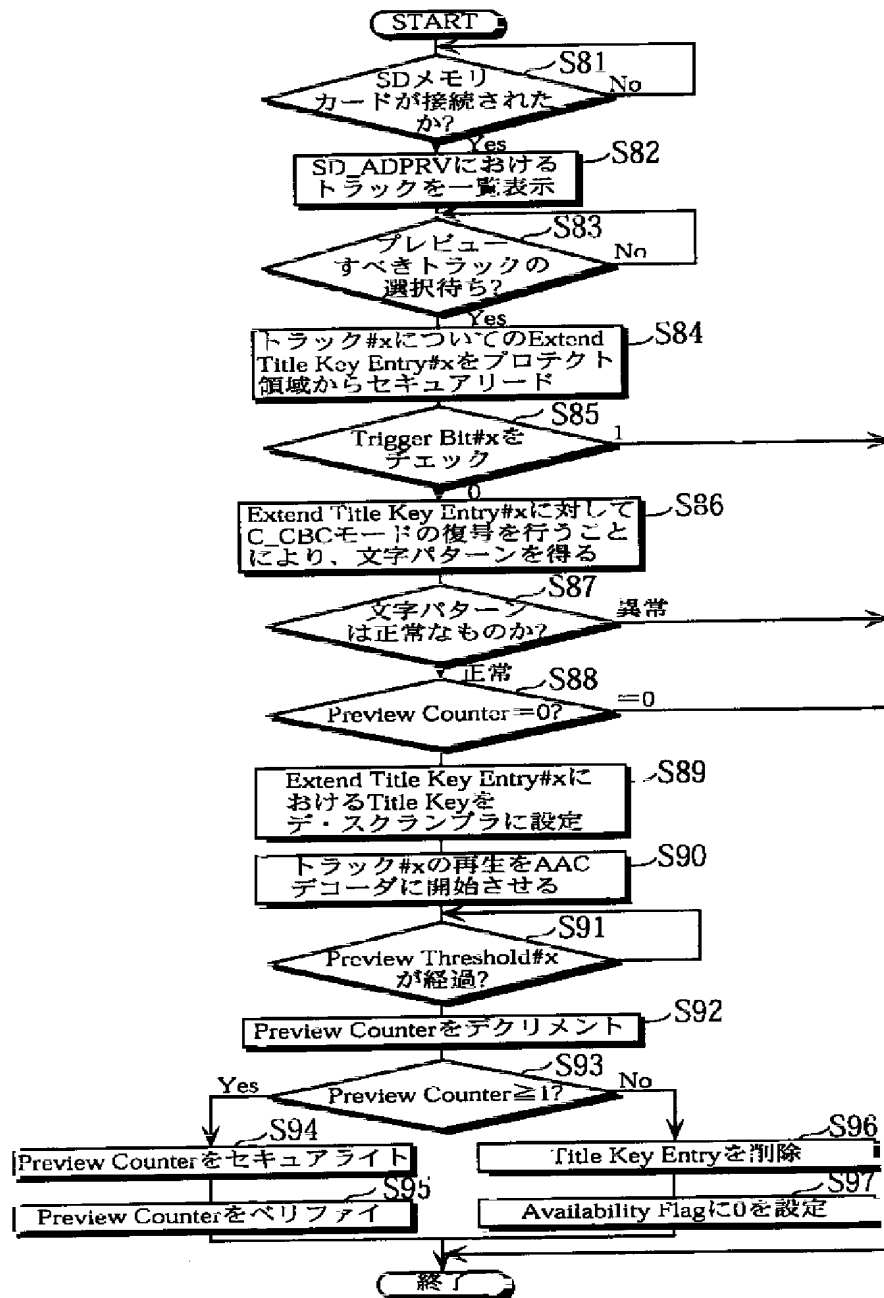
【図41】



【図43】



【図44】



フロントページの続き

(51)Int.Cl.⁷

G 0 6 F 15/00

識別記号

3 1 0

F I

G 0 6 F 15/00

(参考)

3 1 0 A

(31)優先権主張番号 特願2000-125864(P2000-125864)
(32)優先日 平成12年4月26日(2000. 4. 26)
(33)優先権主張国 日本(JP)

(72)発明者 松島 秀樹
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 井上 光啓
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 上坂 靖
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 原田 俊治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 湯川 泰平
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 宮▲ざき▼ 雅也
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 中西 正典
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 小塚 雅之
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) 5B049 AA05 BB11 CC05 CC08 DD01
DD04 EE02 EE28 FF03 FF04
FF06 FF08 GG04 GG07
5B085 AE11 AE23 AE29